REPORTS IN INFORMATICS

ISSN 0333-3590

Generalised Bent Criteria for Boolean Functions

Constanza Riera, George Petrides and Matthew G. Parker

REPORT NO 285 November 2004

Department of Informatics

UNIVERSITY OF BERGEN

Bergen, Norway

This report has URL http://www.ii.uib.no/publikasjoner/texrap/ps/2004-285.ps

Reports in Informatics from Department of Informatics, University of Bergen, Norway, is available at http://www.ii.uib.no/publikasjoner/texrap/.

Requests for paper copies of this report can be sent to:

Department of Informatics, University of Bergen, Høyteknologisenteret,
P.O. Box 7800, N-5020 Bergen, Norway

Generalised Bent Criteria for Boolean Functions

Constanza Riera*, George Petrides†, Matthew G. Parker‡

3rd November 2004

Abstract

We present a generalisation of the Bent property of a boolean function, by proposing spectral analysis with respect to a well-chosen set of local unitary transforms. We relate quadratic boolean functions to quantum error correcting codes and to simple graphs and show that the orbit generated by successive Local Complementations on a graph can be found within the transform spectra under investigation. We also relate the number of flat spectra of a quadratic boolean function to modified versions of its associated adjacency matrix, and develop recursive formulae for the numbers of flat spectra for various quadratic constructions. We also make observations on the generalised Bent properties of boolean functions of algebraic degree greater than two.

1 Introduction

It is often desirable that a boolean function, p, to be used for cryptographic applications, should be highly *nonlinear*, where nonlinearity is determined by examining the spectrum of p with respect to (wrt) the *Walsh Hadamard Transform* (WHT), and where the nonlinearity is maximised for those functions that minimise the magnitude of the spectral coefficients. To be precise, define the boolean function of n variables $p : \mathbb{Z}_2^n \to \mathbb{Z}_2$, and the WHT by the $2^n \times 2^n$ unitary matrix $U = H \otimes H \ldots \otimes H = \bigotimes_{i=0}^{n-1} H$, where the Walsh-Hadamard kernel $H = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix} \right)$, '$\bigotimes$' indicates the tensor product of matrices, and unitary means that $UU^\dagger = I_n$, where '$\dagger$' means transpose-conjugate and I_n is the $2^n \times 2^n$ identity matrix. We further define a length 2^n vector, $s = (s_{00\ldots0}, s_{00\ldots1}, \ldots, s_{11\ldots1})$ such that $s_{\mathbf{i}} = (-1)^{p(\mathbf{x}=\mathbf{i})}$, where $\mathbf{i} \in \mathbb{Z}_2^n$. Then the Walsh-Hadamard spectrum of p is given by the matrix-vector product $P = Us$, where P is a vector of 2^n real spectral coefficients, $P_{\mathbf{k}}$, where $\mathbf{k} \in \mathbb{Z}_2^n$. The spectral coefficient, $P_{\mathbf{k}}$, with maximum magnitude tells us the minimum (Hamming) distance, d, of p to the set of affine boolean functions, where $d = 2^{n-1} - 2^{\frac{n-2}{2}} |P_{\mathbf{k}}|$. By Parseval's Theorem, the extremal case occurs when all $P_{\mathbf{k}}$ have equal magnitude, in which case p is said to have a *flat* WHT spectra, and is referred to as *Bent*. If p is Bent then it is as far away as it can be from the affine functions [31], which is a desirable cryptographic design goal.

*C. Riera is with the Depto. de Álgebra, Facultad de Matemáticas, Universidad Complutense de Madrid, Avda. Complutense s/n, 28040 Madrid, Spain. E-mail: criera@mat.ucm.es

†G.Petrides is with the School of Mathematics, University of Manchester, P.O. Box 88, Sackville Street, Manchester, M60 1QD, UK. E-mail: george.petrides@student.manchester.ac.uk

‡M.G.Parker is with the Selmer Centre, Inst. for Informatikk, Høyteknologisenteret i Bergen, University of Bergen, Bergen 5020, Norway. E-mail: matthew@ii.uib.no. Web: http://www.ii.uib.no/~matthew/

It is an open problem to classify all Bent boolean functions, although many results are known [20, 30, 13, 21]. In this paper we extend the concept of a Bent boolean function to a set of *Generalised Bent Criteria* for a boolean function, where we now require that p has flat spectra wrt one or more transforms from a specified set of unitary transforms. The set of transforms we choose is not arbitrary but is motivated by the choice of unitary transforms that are typically used to action a local basis change for a pure n-qubit quantum state. We here apply such transforms to a n-variable boolean function, and examine the resultant spectra accordingly. In particular we apply all possible transforms formed from n-fold tensor products of the Identity $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right)$, the Walsh-Hadamard kernel, H, and the Negahadamard kernel [33], $N = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & i \\ 1 & -i \end{smallmatrix} \right)$, where $i^2 = -1$. We refer to this set of transforms as the $\{I, H, N\}^n$*transform set*, i.e. where all transforms are of the form $\bigotimes_{i=0}^{n-1} \{I, H, N\}$, where each member of the set is an n-fold tensor product of members of the set $\{I, H, N\}$. There are 3^n such transforms which act on a boolean function of n variables to produce 3^n spectra, each spectrum of which comprises 2^n spectral elements (complex numbers). By contrast, the WHT can be described as $\{H\}^n$, which is a transform set of size one, where the single resultant output spectrum comprises just 2^n spectral elements. It has recently been shown that spectral analysis wrt the $\{I, H, N\}^n$ transform set has application, not just in the context of quantum systems, but also in the context of the cryptanalysis of classical cryptographic systems [17]. In particular, for a block cipher it models attack scenarios where one has full read/write access to a subset of the plaintext bits and access to all ciphertext bits, (see [17] for more details). The analysis of spectra wrt $\{I, H, N\}^n$ can tell us more about p than is provided by just the spectrum wrt the WHT, for instance, identifying relatively higher generalised linear biases for p [37]. The choice of I, H, and N, is also motivated by their importance for the construction of *Quantum Error-Correcting Codes* (QECCs). This is because they are generators of the *Local Clifford Group* [11, 29] which is defined to be the set of matrices that *stabilize* the group of Pauli matrices which, in turn, form a basis for the set of local errors that act on the quantum code. This implies that the set of *locally-equivalent* quantum states, that occur as joint eigenspectra wrt $\{I, H, N\}^n$, are equally robust to quantum errors from the Pauli error set. To evaluate the quantum *entanglement* of a pure multi-qubit state one should really examine the spectra wrt the infinite set of order-n tensor products of all 2×2 unitary matrices [35]. Those states which minimise all spectral magnitudes wrt this infinite transform set are as far away as possible from all generalised affine functions and can be considered to be highly entangled as the probability of observing (measuring) any specific qubit configuration is as small as possible, in any local measurement basis. However it is computationally intractable to evaluate, to any reasonable approximation, this continuous local unitary spectrum beyond about $n = 3$ qubits (although approximate results up to $n = 6$ are given in [35]). Therefore we choose, in this paper, a well-spaced subset of spectral points, as computed by the set of $\{I, H, N\}^n$ transforms, from which to ascertain approximate entanglement measures. Complete spectra for such a transform set can be computed up to about $n = 10$ qubits using a standard desk-top computer, although partial results for significantly higher n are possible if the quantum state is represented by, say, a quadratic boolean function. In this paper one is interested, particularly, in the location and number of flat spectra wrt $\{I, H, N\}^n$. Very loosely, for p of fixed algebraic degree, the more flat (or near-flat) spectra $p$has wrt $\{I, H, N\}^n$, the stronger it is in a cryptographic sense, and also the more *entangled* it is when interpreted as a quantum state [35, 27] - of course one should consider these measures of cryptographic strength and/or entanglement as only partial. In cryptographic terms we are trying to answer the question: which functions are as far away as possible from the set of generalised affine functions as

defined by the rows of the $\{I, H, N\}^n$ set? [1]

Although the classification of Bent quadratic (degree-two) boolean functions is well-known [30], the classification of generalised Bent criteria for a quadratic boolean function wrt the $\{I, H, N\}^n$ transform set is new. This paper provides new results for both quadratic and more general boolean functions. In particular, we associate a quadratic boolean function with an undirected graph, which allows us to interpret spectral flatness with respect to $\{I, H, N\}^n$ as a maximum rank property of suitably modified adjacency matrices. The graphical description of certain pure quantum states was investigated by Parker and Rijmen [35]. They also proposed partial entanglement measures for such states and made observations about a *Local Unitary (LU) Equivalence* between graphs describing the states wrt the tensor product of 2×2 local unitary transforms. These graphs were interpreted as quadratic boolean functions and it was also noted that bipartite quadratic functions are LU-equivalent to binary linear error-correcting codes. It was further observed that physical quantum graph arrays were relevant to the work of [35] and were already the subject of active investigation, as described by the *cluster states* of Raussendorf and Briegel [38, 6], these clusters forming the 'substrate' for measurement-driven quantum computation. Measurement-driven quantum computation on a *quantum factor graph* has also been discussed by Parker [34]. Independent work by Schlingemann and Werner [40], Glynn [22, 23], and by Grassl, Klappenecker, and Rotteler [25] proposed to describe *stabilizer* Quantum Error-Correcting Codes (QECCs) using graphs and, for QECCs of dimension zero, the associated graphs can be referred to as *graph states*. It is apparent that these graph states are equivalent to the graphs described by [35] and, therefore, that graph states have a natural representation using quadratic boolean functions. Stabilizer QECCs can also be interpreted as additive codes over GF(4) [11]. LU-equivalences between certain graph states were observed in [35], in particular that the complete graph, the star graph, and the generalised GHZ (Greenberger-Horne-Zeilinger) states are all LU-equivalent. It turns out that LU-equivalence for graph states can be characterised, graphically, via the *Vertex-Neighbour-Complement* (VNC) transformation, which was defined by Glynn, in the context of QECCs, in [22] (definition 4.2) and also, independently, by Hein, Eisert and Briegel [27], and also by Van Den Nest and De Moor [43]. VNC is another name for *Local Complementation* (LC), as investigated by Bouchet [7, 8, 9] in the context of *isotropic systems*. There has been some recent renewed interest in Bouchet's work motivated, in part, by the application of *interlace graphs* to the reconstruction of DNA strings [3, 2]. In particular, various *interlace polynomials* have been defined [2, 1, 4, 5] which mirror some of the quadratic results of this paper. We will point out some links to this work as we go along although we defer a thorough exposition of these links to future work. This paper answers, to some extent, a question posed at the end of [4] as to a simple combinatorial explanation of the interlace polynomial q. It is apparent from our paper that q summarises some of the spectral properties of the graph wrt the $\{I, H\}^n$ transform set (this transform set was also examined in [35]). Similarly the interlace polynomial Q, as defined in [1], summarises some of the spectral properties of the graph wrt the $\{I, H, N\}^n$ transform set. Furthermore our paper provides a natural setting for future investigations into the generalisation of the interlace polynomial to hypergraphs.

[1] A row of $U_0 \otimes U_1 \otimes \ldots \otimes U_{N-1}$ for U_i a 2×2 unitary matrix can always be written as $u = (a_0, b_0) \otimes (a_1, b_1) \otimes \ldots \otimes (a_{n-1}, b_{n-1})$, where a_i, b_i are complex numbers. For α a Pth complex root of 1, and M an integer modulus, we can approximate a normalised version of u by $u \simeq m(\mathbf{x})\alpha^{p(\mathbf{x})}$, for some appropriate choice of integers $M$and P, where $m : \mathbb{Z}_2^n \to \mathbb{Z}_M$, $p : F_2^n \to \mathbb{Z}_P$, and $\mathbf{x} \in \mathbb{Z}_2^n$, such that the ith element of u, $u_i = m(\mathbf{x} = \mathbf{i})\alpha^{p(\mathbf{x}=\mathbf{i})}$, where $\mathbf{i} \in \mathbb{Z}_2^n$ and u_i is interpreted as a complex number. When u is fully-factorised using the tensor product then m and p are affine functions and we say that u represents a generalised affine function (see [35], Section 5, for more details).

By applying the LC operation to a graph G we obtain a graph G', in which case we say that G and G' are *LC-equivalent*). LC-equivalence translates into the natural equivalence between GF(4) additive codes that keeps the weight distribution of the code invariant [11]. In this paper we interpret LC as an operation on quadratic boolean functions, and as an operation on the associated graph adjacency matrix, and we also identify the LC orbit with a subset of the flat spectra wrt the $\{I, H, N\}^n$ transform set. It is the spectral context of LC that motivates us to investigate some more general spectral properties of boolean functions, as discussed earlier. The spectra wrt the $\{I, H, N\}^n$transform set includes the examination of the properties of the WHT of all $\mathbb{Z}_4$-linear offsets of boolean functions, the WHT of all the subspaces of boolean functions that can be obtained by fixing a subset of the variables, the WHT of all $\mathbb{Z}_4$-linear offsets of all of the above subspace boolean functions, the WHT of each member of the LC orbit, and the distance of boolean functions to all $\mathbb{Z}_4$-linear functions. This leads us to prove the following:

All quadratic boolean functions are *Bent*$_4$, *IBent* and *IBent*$_4$.
Not all quadratic boolean functions are *LC-Bent*.
All boolean functions are *IBent*$_4$.
Not all boolean functions are *Bent*$_4$ or *IBent*.
There are no $\mathbb{Z}_4$-*Bent* or *Completely IBent*$_4$ boolean functions.

where the above terms for generalised Bent criteria will be made clear in the sequel. We further prove that, for certain recursive quadratic boolean constructions, one can establish simple recursive relationships for the number of flat spectra wrt the $\{I, H, N\}^n$ transform set. In all cases we are able to characterise and analyse the criteria for quadratic boolean functions by considering properties of the associated adjacency matrix for the graph state.

In Section 2 we briefly review the graph state and its intepretation as a zero-dimension QECC, as a self-dual additive code over GF(4), as a self-dual additive code over $\mathbb{Z}_4$, as an isotropic system, and as a quadratic boolean function. Finally we note that bipartite graphs have an interpretation as binary linear error-correcting codes which is made explicit via the quadratic boolean function representation.

In Section 3 we review the LC operation as an operation on an undirected graph, as described by [22, 23], and we provide an algorithm for LC in terms of the adjacency matrix associated with the graph.

In Section 4, we show that the LC orbit for a quadratic boolean function lies within the set of transform spectra wrt tensor products of the 2×2 identity matrix, I, $\sqrt{-i\sigma_x}$, and $\sqrt{i\sigma_z}$, where σ_x and σ_z are Pauli matrices. We also show that, equivalently, the orbit lies within the transform set wrt $\{I, H, N\}^n$. We show that doing LC to the vertex (equivalently, variable) x_v can be realised by the application of the Negahadamard kernel, N, to position v (and the identity matrix to all other positions) of the bipolar vector $(-1)^{p(\mathbf{x})}$, i.e.

$$(-1)^{p'(\mathbf{x})} \simeq U_v(-1)^{p(\mathbf{x})} = I \otimes \cdots \otimes I \otimes N \otimes I \otimes \cdots \otimes I \ (-1)^{p(\mathbf{x})}$$

where $p'(\mathbf{x})$ is the function after applying LC to variable x_v, and '$\simeq$' indicates equality of vectors to within some affine offset of $p'(\mathbf{x})$, over $\mathbb{Z}_8^n$. We then find the general formula, mod 4, for the action of one LC step on a boolean function of any degree. Finally we identify spectral symmetries that hold for $p(\mathbf{x})$ of any degree wrt $\{I, H, N\}^n$.

In Section 5, we introduce the concepts of *Bent*$_4$, $\mathbb{Z}_4$-*Bent*, *(Completely) IBent*, *LC-Bent*, and *(Completely) IBent*$_4$ boolean functions, and we show how, for quadratic

boolean functions, these properties can be evaluated by examining the ranks of suitably modified versions of the adjacency matrix of a boolean quadratic function. These modifications are directly related to the application of transforms from the set $\{I, H, N\}^n$. We also prove simple recursions for the number of flat spectra of certain boolean constructions wrt the $\{I, H, N\}^n$ transform set, or subsets thereof, and we also observe that optimal QECCs, interpreted as quadratic boolean functions, appear to maximise the number of flat spectra wrt $\{I, H, N\}^n$.

2 The Graph States

In this section we briefly characterise graph states in a number of ways. It is surprising how many different characterisations exist for these objects in the literature.

2.1 Interpretation as a Quantum Error Correcting Code

Let E be a $2n$-dimensional binary vector space, whose elements are written as $(a|b)$, equiped with the (symplectic) inner product $((a|b),(a'|b')) = a \cdot b' + a' \cdot b$. Define the weight of $(a|b) = (a_1, \ldots, a_n|b_1, \ldots, b_n)$ as the number of coordinates i such that at least one of the a_i or b_i is 1. The distance between two elements $(a|b)$ and $(a'|b')$ is defined to be the weight of their difference. From [11], we have the following theorem:

Theorem 1. *[11] Let S be a $(n-k)$ - dimensional linear subspace of E, contained in its dual $S^\perp$ (with respect to the inner product), and such that there are no vectors of weight $< d$ in $S \setminus S^\perp$. Then, by taking an eigenspace of S (for any chosen linear character) we obtain a quantum error-correcting code mapping k qubits to n qubits that can correct $[(d-1)/2]$ errors. Such a code will be called an* additive quantum error-correcting code (QECC)*, and it is described by its parameters, $[[n, k, d]]$, where d is the* minimal distance *of the code.*

We show, later, that a $[[n, 0, d]]$ QECC can be represented by a graph. First we re-express the QECC as a GF(4) additive code.

2.2 Interpretation as a GF(4) Additive Code

From [11] we see how to interpret the binary space E as the space $\mathrm{GF}(4)^n$ and thereby how to derive a QECC from an additive (classical) code over $\mathrm{GF}(4)^n$:

Let $GF(4) = \{0, 1, \omega, \bar{\omega}\}$, with $\omega^2 = \omega + 1$, $\omega^3 = 1$; and conjugation defined by $\bar{\omega} = \omega^2 = \omega + 1$. The *Hamming weight* of a vector in $\mathrm{GF}(4)^n$, written $wt(u)$, is the number of non-zero components, and the *Hamming distance* between $u, u' \in \mathrm{GF}(4)^n$ is $\mathrm{dist}(u, u') = wt(u+u')$. We define the *trace function* as: $tr(x) : GF(4) \to GF(2)$, $tr(x) = x + \bar{x}$. To each vector $v = (a|b) \in E$ we associate the vector $\phi(v) = a\omega + b\bar{\omega}$. By this association we see that the weight of v is the Hamming weight of $\phi(v)$, and that the distance between two vectors in E is the Hamming distance of their images. Now, if S is a subspace of E then $C = \phi(S)$ is a subset of $\mathrm{GF}(4)^n$ that is closed under addition (defining thus an additive code). Defining the *trace inner product* of $u, v \in \mathrm{GF}(4)^n$ as

$$u \star v = Tr(u \cdot \bar{v}) = \sum_{i=1}^{n} (u_i \bar{v_i} + \bar{u_i} v_i)$$

we can define the *dual code* $C^{\perp}$ as

$$C^{\perp} = \{u \in \ \mathrm{GF}(4)^n : u \star v = 0 \ \forall v \in C\}$$

Now one can reformulate Theorem 1.

Theorem 2. *Let C be an additive self-orthogonal subcode of $GF(4)^n$, containing 2^{n-k} vectors, such that there are no vectors of weight $< d$ in $C \setminus C^{\perp}$. Then any eigenspace of $\phi^{-1}(C)$ is a QECC with parameters $[[n, k, d]]$.*

By Glynn (see [22, 23]), we have: Let S be a stabilizer matrix ($Su = u \ \forall u$), that is $(n-k) \times n$ over GF(4) and such that its rows are GF(2)-linearly independent. Then we can define a QECC with parameters $[[n, k, d]]$ as the set of all GF(2)-linear combinations of the rows of S. We call the code *self-dual* when $k = 0$.

2.3 The QECC as a Graph

We are going to assume that each column of S contains at least two non-zero values, for the columns that do not have this property may be deleted to obtain a better code. Following [22], we also see that a self-dual quantum code $[[n, 0, d]]$ corresponds to a graph on n vertices, which may be assumed to be connected if the code is indecomposable:

Let $\mathrm{PG}(m, q)$ be the finite projective space defined from the vector space of rank $m+1$ over the field $\mathrm{GF}(q)$. Then, the *Grassmannian* of lines of $\mathrm{PG}(n-1, 2)$, $G_1(\mathrm{GP}(n-1, 2)$, regarded as a variety immersed in $\mathrm{PG}(\binom{n}{2}, 2)$ is as follows: each line l_i is defined by two points, a_i and b_i. Then we associate to the set of lines all products $a_i b_j + a_j b_i, \ i \neq j \ (\mathrm{mod} 2)$.

We can define a mapping from a column of an $n \times n$ stabilizer matrix S over GF(4) to a vector of length $\binom{n}{2}$ with coefficients in GF(2): first we write each column over GF(4) as $a + b\omega, \ a, b \in \mathrm{GF}(2)^n$. Then, we get

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \omega \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

Taking all the 2×2 subdeterminants found when we put the two vectors into a matrix, we get the points of the Grassmannian. We have:

A point in $G_1(\mathrm{GP}(n-1, 2)) \equiv$ a line in $\mathrm{GP}(n-1, 2) \equiv$ a column of length n over GF(4) (with at least two different non-zero components). Then a quantum self-dual code $[[n, 0, d]]$ corresponds to some set of n lines that generate $\mathrm{PG}(n-1, 2)$. As each line of $\mathrm{PG}(n-1, 2)$ corresponds to a (star) kind of graph, the set corresponds to a certain graph in n vertices.

2.4 Interpretation as a Modified Adjacency Generator Matrix over GF(2) and GF(4)

From any connected graph we can obtain an indecomposable code:

Let Γ be the adjacency matrix of a graph G in n variables. Then, $G_T = (I \mid \Gamma)$ (where I is the $n \times n$ identity matrix) is the generator matrix of a binary linear code (see Tonchev [42]). That is,

$$G_T = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 & a_{01} & \dots & a_{0n} \\ 0 & 1 & 0 & \dots & 0 & a_{01} & 0 & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & a_{0n} & a_{1n} & \dots & 0 \end{pmatrix}$$

generates a code over $\mathrm{GF}(2)^n$. We can interprete further this as a generating matrix of a code over $\mathrm{GF}(4)^n$ (see [11]), as follows:

$$G = \Gamma + \omega I = \begin{pmatrix} \omega & a_{01} & \dots & a_{0n} \\ a_{01} & \omega & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{0n} & a_{1n} & \dots & \omega \end{pmatrix}$$

is the generating matrix of an additive code over $\mathrm{GF}(4)^n$. Different graphs may define the same QECC, but this relation is 1-1 with respect to LC-equivalence between graphs, as defined in section 3.

2.5 Interpretation as a Modified Adjacency Matrix over $\mathbb{Z}_4$

We can equivalently define, from a graph with adjacency matrix Γ, the generating matrix of an additive code over $\mathbb{Z}_4^n$ as $2\Gamma + I$. This code has the same weight distribution over $\mathbb{Z}_4^n$ as $\Gamma + \omega I$ over $\mathrm{GF}(4)^n$. Once again, LC-equivalent graphs define equivalent QECCs and their associated modified adjacency matrices over $\mathbb{Z}_4$ define additive codes over $\mathbb{Z}_4$ with the same weight distribution.

2.6 Interpretation as an Isotropic System

The graph state can also be viewed as an isotropic system (see [7, 9, 8, 14, 32]).

Let A be a 2-dimensional vector space over $\mathrm{GF}(2)$. For $x, y \in A$, define a bilinear form, $<,>$, by

$$< x, y >= \begin{cases} 1 & \text{if } x \neq y, x \neq 0 \text{ and } y \neq 0 \\ 0, & \text{otherwise} \end{cases}$$

Let V be a finite set. Then we can define the space of $\mathrm{GF}(2)$-homomorphisms $A^V : V \to A$. We define in this $\mathrm{GF}(2)$-vector space a bilinear form as:

$$\text{for } \phi, \psi \in A^V, \ < \phi, \psi >= \sum_{v \in V} < \phi(v), \psi(v) > \pmod 2$$

Definition 1. *Let L be a subspace of A^V. Then, $I = (V, L)$ is an* isotropic system *if dim $(L) = |V|$ and $< \phi, \psi >= 0 \ \forall \phi, \psi \in L$.*

We can now see how we relate a graph to an isotropic system:

For a graph G, $V(G)$ denotes the set of vertex of G. If $v \in V(G)$, $\mathcal{N}(v)$ denotes the *neighborhood* of the vertex v, that is, the set of all its neighbors. For $P \subseteq V$, we set $\mathcal{N}(P) = \sum_{v \in P} \mathcal{N}(v)$. Let $K = \{0, x, y, z\}$ be the Klein group, which is a 2-dimensional vector space, and set $K' = K \setminus \{0\}$. We note that $x + y + z = 0$. Then,

Lemma 1. *([9]) Let G be a simple graph with vertex set V. Let $\phi, \psi \in K'^V$ such that $\phi(v) \neq \psi(v)\ \forall v \in V$, and set $L = \{\phi(P) + \psi(\mathcal{N}(P)) \ : \ P \subseteq V\}$. Then $S = (L, V)$ is an isotropic system.*

The triple $\Pi = (G, \phi, \psi)$ is called a *graphic presentation* of S.

For $\phi \in K^V$, we set $\widehat{\phi} = \{\phi(P) \ : \ P \subseteq V\}$. We note that $\widehat{\phi}$ is a vector subspace of K^V.

Definition 2. *For $\psi \in K'^V$, the restricted Tutte-Martin polynomial $m(S, \psi; x)$ is defined by*

$$m(I, \psi; x) = \sum (x-1)^{dim(L \cup \widehat{\phi})},$$

where the sum is over $\phi \in K'^V$ such that $\phi(v) \neq \psi(v),\ v \in V$.

Then,

Theorem 3. *([9]) If G is a simple graph and I is the isotropic system defined by a graphic presentation (G, ϕ, ψ), then*

$$q(G; x) = m(I, \phi + \psi; x),$$

where $q(G; x)$ is the interlace polynomial of G.

We'll discuss in later sections the interlace polynomial and its relation to our work.

2.7 Interpretation as a Quadratic Boolean Function

We can also interpret a quadratic Boolean function as a non-directed graph (and viceversa), as seen in [35], in the following way: Let $p(\mathbf{x}) : F_2^n \to F_2$ be a quadratic boolean function, defined by its Algebraic Normal Form (ANF),

$$p(\mathbf{x}) = \sum_{0 \leq i < j \leq n-1} a_{ij} x^i x^j + \sum_{i=0}^{n-1} b_i x_i + \sum_{i=0}^{n-1} c_i$$

Then we can associate to it the non-directed graph that has as vertices the variables, considering that two vertices x_i, x_j are connected iff the term $x_i x_j$ appears in the ANF of the function. Only quadratic terms are required to construct the graph (we obtain only simple graphs), and the function and the graph are in 1-1 correspondence, but for an affine offset. As a graph, it has an adjacency matrix, defined as Γ, such that $\Gamma(i, j) = \Gamma(j, i) = a_{ij}$, $i < j$, $\Gamma(i, i) = 0$. That is,

$$\Gamma = \begin{pmatrix} 0 & a_{01} & a_{02} & \dots & a_{0n} \\ a_{01} & 0 & a_{12} & \dots & a_{1n} \\ a_{02} & a_{12} & 0 & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{0n} & a_{1n} & a_{2n} & \dots & 0 \end{pmatrix}$$

2.8 Interpretation of a Bipartite Quadratic Boolean Function (bipartite graph) as a Binary Linear Code

In [35] we see that quadratic ANFs, as represented by bipartite graphs, have an interpretation as binary linear codes: Let $\mathbf{T_C}$, $\mathbf{T_{C^\perp}}$ be a bipartite splitting of

$\{0,\ldots,n-1\}$, and let us partition the variable set $\mathbf{x}$ as $\mathbf{x} = \mathbf{x_C} \cup \mathbf{x_{C^\perp}}$, where $\mathbf{x_C} = \{x_i : i \in \mathbf{T_C}\}$, and $\mathbf{x_{C^\perp}} = \{x_i : i \in \mathbf{T_{C^\perp}}\}$. Then, if we have a function of the form $p(\mathbf{x}) = \sum_k q_k(\mathbf{x_C}) r_k(\mathbf{x_{C^\perp}})$, where $\deg(q_k(\mathbf{x_C})) = \deg(r_k(\mathbf{x_{C^\perp}})) = 1\ \forall k$ (clearly, such a function corresponds to a bipartite graph), and we define $s(\mathbf{x}) = (-1)^{p(\mathbf{x})}$, the action of the transform $\bigotimes_{i\in\mathbf{T}} H_i$, with $\mathbf{T} = \mathbf{T_C}$ or $\mathbf{T_{C^\perp}}$, on the form $s(\mathbf{x})$ gives $s'(\mathbf{x}) = m(\mathbf{x})$, with m the ANF of a Boolean function. s' is the binary indicator for a binary linear $[n, n-|\mathbf{T}|, d]$ error correcting code (where H_i, say, is short for $I \otimes I \otimes \ldots \otimes H \otimes \ldots \otimes I$ with H in the ith position). [2]

3 Local Complementation (LC)

Given a graph G with adjacency matrix Γ, we define its *complement* to be the graph with adjacency matrix $\Gamma + I + \mathbf{1}(\bmod 2)$, where I is the identity matrix and $\mathbf{1}$ is the all-ones matrix.

Definition 3. *We define the action of* LC *(or* vertex-neighbour-complement (VNC)*) on a graph G at vertex v as the graph transformation obtained by replacing the subgraph $G[\mathcal{N}(v)]$ (i.e., the induced subgraph of the neighbourhood of the vth vertex of G) by its complement.*

By Glynn (see [22]), a self-dual quantum code $[[n, 0, d]]$ corresponds to a graph on n vertices, which may be assumed to be connected if the code is indecomposable. It is shown there that two graphs G and H give equivalent self-dual quantum codes if and only if H and G are LC-equivalent.

For a study of the group of compositions of local complementations, see [7, 9, 8, 14], which describe the relation between local complementation and *isotropic systems*. Essentially, a suitably-specified isotropic system has graph presentations G and G' iff G and G' are locally equivalent wrt local complementation.

3.1 LC in terms of the adjacency matrix

Let $p(\mathbf{x}) : F_2^n \to F_2$ be a (homogeneous) quadratic boolean function, defined by,

$$p(\mathbf{x}) = \sum_{i<j} a_{ij} x^i x^j$$

As we have seen, we can express it by the adjacency matrix of its associated graph, Γ, such that $\Gamma(i,j) = \Gamma(j,i) = a_{ij}$, $i < j$, $\Gamma(i,i) = 0$. The LC operation on the graph associated to $p(\mathbf{x})$ can be expressed by means of a simple algorithm in terms of the adjacency matrix. Without loss of generality, we show how the matrix changes from Γ to Γ_0 after doing LC on vertex x_0:

$$\Gamma_0 = \begin{pmatrix}
0 & a_{01} & a_{02} & a_{03} & \ldots & a_{0n} \\
a_{01} & 0 & a_{12}+a_{01}a_{02} & a_{13}+a_{01}a_{03} & \ldots & a_{1n}+a_{01}a_{0n} \\
a_{02} & a_{12}+a_{01}a_{02} & 0 & a_{23}+a_{02}a_{03} & \ldots & a_{2n}+a_{02}a_{0n} \\
a_{03} & a_{13}+a_{01}a_{03} & a_{23}+a_{02}a_{03} & 0 & \ldots & a_{3n}+a_{03}a_{0n} \\
\ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\
a_{0n} & a_{1n}+a_{01}a_{0n} & a_{2n}+a_{02}a_{0n} & a_{3n}+a_{03}a_{0n} & \ldots\ldots & 0
\end{pmatrix}$$

[2] There is also an equivalent interpretation of bipartite graphs as *binary matroids* (e.g. [12]).

The general algorithm, mod 2, is

$$\begin{cases} \Gamma_v(i,j) = \Gamma(i,j) + \Gamma(v,i) * \Gamma(v,j), & i < j, \quad i,j = 1,...,n \\ \Gamma_v(i,i) = 0 \quad \forall i \\ \Gamma_v(j,i) = \Gamma_v(i,j), & i > j \end{cases}$$

where Γ_v is the adjacency matrix of the function after doing LC to the vertex x_v.

Proof. We look at the ANF of the function. Applying LC to vertex x_v only affects the relations between its neighbours. That is, it changes the relations of x_i if and only if this vertex is a neighbour of x_v (i.e., if and only if $a_{vi} = a_{iv} = 1$). We thus have two cases:

1) $a_{vi} = 0 \Rightarrow a^v_{ij} = a_{ij} \quad \forall j = 1,...,n,$ where $a_{ij} = \Gamma(i,j), \quad a^v_{ij} = \Gamma_v(i,j)$

2) $a_{vi} = 1 \Rightarrow a^v_{ij} = a_{ij}$ if $a_{vj} = 0$; $a^v_{ij} = a_{ij} + 1$ if $\begin{cases} a^v_{ij} = a_{ij} & \text{if } a_{vj} = 0 \\ a^v_{ij} = a_{ij} + 1 & \text{if } a_{vj} = 1 \end{cases}$

Finally, we can write this in a neater way, saying that $a^v_{ij} = a_{ij} + a_{vi}a_{vj}$. We obtain the deduced algorithm by writing the above as a matrix. □

4 Local Complementation (LC) and Local Unitary (LU) Equivalence

Hein et al [27] state that Local Unitary (LU) Equivalence of graph states is obtained via successive transformations of the form,

$$U_v(G) = (-i\sigma_x^{(v)})^{1/2} \prod_{b \in \mathcal{N}_v} (i\sigma_z^{(b)})^{1/2} \tag{1}$$

where $\sigma_x = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right)$ and $\sigma_z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix} \right)$ are Pauli matrices, the superscript (v) indicates that the Pauli matrix acts on qubit v (with Iacting on all other qubits), and $\mathcal{N}_v$ comprises the neighbours of qubit v in the graphical representation [3]. Define matrices $x$and $z$as follows,

$$x = (-i\sigma_x)^{1/2} = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & i \\ i & -1 \end{pmatrix}$$

and

$$z = (i\sigma_z)^{1/2} = \begin{pmatrix} w & 0 \\ 0 & w^3 \end{pmatrix}$$

where $w = e^{2\pi i/8}$. Furthermore, let $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right)$.

Let us further define the set, $\mathbf{D}$ to be the set of 2×2 diagonal or anti-diagonal local unitary matrices, i.e. of the form $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix} \right)$ or $\left(\begin{smallmatrix} 0 & a \\ b & 0 \end{smallmatrix} \right)$, for some a and b. We make extensive use of the fact that a final multiplcation of a spectral vector by tensor products of members of $\mathbf{D}$ does not change the spectral coefficient magnitudes. In this sense a final multiplication by tensor products of members of $\mathbf{D}$ has no effect on the final spectrum. For instance, applying $x$twice to the same qubit is the same as applying $x^2 = \left(\begin{smallmatrix} 0 & -i \\ -i & 0 \end{smallmatrix} \right)$, which is in $\mathbf{D}$, and it is therefore apparent that applying x^2 to any specific qubit of a graph G maintains the graph spectrum as flat and, moreover, does not alter the underlying graphical interpretation if we ignore all final

[3] The other two Pauli matrices are $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right)$ and $\sigma_y = i\sigma_x\sigma_z = \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix} \right)$

trivial transforms by the tensor product of matrices from $\mathbf{D}$. Therefore we can, to within such trivial final transformations, equate x^2 with the identity matrix, i.e. $x^2 \simeq I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right)$. By similar argument, the action of any 2×2 matrix from the set, $\mathbf{D}$, of diagonal or anti-diagonal matrices on a specific qubit is, to within a trivial final transformation, the action of the identity matrix on the same qubit. Note also that $z \in \mathbf{D}$. The same equivalence holds over n qubits, so we can define an equivalence relation with respect to a tensor product of members of $\mathbf{D}$ by the symbol '$\simeq$'. Let u and v be two 2×2 unitary matrices. Then,

$$u \simeq v \quad \Leftrightarrow \quad u = dv, \qquad d \in \mathbf{D}$$

This equivalence relation allows us to simplify the concatenation of actions of $x$and z on a specific qubit. Thus, for instance, $z \simeq I$.

Lemma 2. *Given any u, v in $\mathbf{D}$, and any 2×2 unitary matrix, w,*

$$\begin{array}{ll} & uw \simeq vw \simeq w \\ \not\Rightarrow & wu \simeq wv \end{array}$$

We now show that the LC orbit is found within the transform spectra with respect to the transform set, I, x, and xz. Subsequently, it will be shown that we can alternatively find the LC orbit within the transform set defined by I, H and N, where H is the Walsh-Hadamard kernel, $H = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix} \right)$, and $N$is the Negahadamard kernel [33], $N = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & i \\ 1 & -i \end{smallmatrix} \right)$. We then re-derive the single LC operation on a graph from the application of x (or N) on a single qubit, and discuss extensions of the application of LC to boolean functions of degree higher than two.

4.1 The LC Orbit Occurs Within the $\{I, x, xz\}^n$ Set of Transform Spectra

By applying $U_v(G)$successively for various v to an initial state, one can generate all LU-equivalent graphs within a finite number of steps. (It is immediately evident from the action of LC on a graph that any LC orbit must be of finite size). Instead of applying U successively, it would be nice to identify a (smaller) transform set in which all LU-equivalent graphs exist as the spectra, to within a post-multiplication by the tensor product of matrices from $\mathbf{D}$.

Lemma 2 tells us that $zx \simeq x$, and $zxx \simeq I$. Furthermore, it is easy to verify, computationally, that,

Lemma 3. $xzx \simeq zxz$

With these above definitions and observations we can derive the following theorem.

Theorem 4. *To within subsequent transformation by tensor products of matrices from $\mathbf{D}$, the LC orbit of the graph, G, over $n$qubits occurs within the spectra of all possible tensor product combinations of the 2×2 matrices, I, x, and xz. There are 3^nsuch transform spectra.*

Proof. For each specific qubit in G, consider every possible product of the two matrices, x, and z. Using the equivalence relationship defined earlier, and Lemmas 2 and 3,

- $xxx \simeq x$
- $xxz \simeq I$
- $xzx \simeq zxz \simeq xz$
- $xzz \simeq zxzz \simeq xzxz \simeq xxzx \simeq x$
- $zxx \simeq I$
- $zxz \simeq xz$
- $zzx \simeq x$
- $zzz \simeq I$

Thus any product of three or more instances of x and/or z can always be reduced to I, x, or xz. Theorem 4 follows by recursive application of (1) with these rules, and by noting that the rules are unaffected by the tensor product expansion over n qubits. □

For instance, for $n = 2$, the LC orbit of the graph represented by the quadratic function $p(\mathbf{x})$ is found as a subset of the $3^2 = 9$ transform spectra of $(-1)^{p(\mathbf{x})}$: $I \otimes I$, $I \otimes x$, $I \otimes xz$, $x \otimes I$, $x \otimes x$, $x \otimes xz$, $xz \otimes I$, $xz \otimes x$, and $xz \otimes xz$.

Theorem 4 gives a trivial and very loose upper bound on the maximum size of any LC orbit over n qubits, this bound being 3^n. It has been computed in [16] that the number of LC orbits for connected graphs for $n = 1$ to $n = 12$ are $1, 1, 1, 2, 4, 11, 26, 101, 440, 3132, 40457$, and 1274068, respectively (see also [27, 23, 28, 15, 41]).

4.2 The LC Orbit Occurs Within the $\{I, H, N\}^n$ Set of Transform Spectra

One can verify, computationally, that $N \simeq x$ and $H \simeq xz$. Therefore one can replace x and xz with N and H, respectively, so that the transform set, $\{I, xz, x\}$ becomes $\{I, H, N\}$. This is of theoretical interest because H defines a 2-point (periodic) Discrete Fourier Transform matrix, and N defines a 2-point negaperiodic Discrete Fourier Transform matrix. In other words, this basis change from the rows of x and xz to the rows of N and H may provide a more natural set of multidimensional axes in some contexts. For t a non-negative integer,

$$N^{3t} \simeq I, \qquad N^{3t+1} \simeq N, \qquad N^{3t+2} \simeq H, \qquad N^{24} = I \tag{2}$$

so N could be considered a 'generator' of $\{I, H, N\}$. The $\{I, H, N\}^n$ transform set over n binary variables has been used to analyse the resistance of certain S-boxes to a form of Generalised Linear Cryptanalysis in [37]. It also defines the basis axes under which aperiodic autocorrelation of boolean functions is investigated in [17]. The *Negahadamard Transform*, $\{N\}^n$, was introduced in [33]. Constructions for boolean functions with favourable spectral properties wrt the $\{H, N\}^n$ transform (amongst others) have been proposed in [36], and [35] showed that boolean functions that are LU-equivalent to distance-optimal binary error-correcting codes yield favourable spectral properties wrt the $\{I, H\}^n$ transform.

4.3 A Spectral Derivation of LC

We now re-derive LC by examining the repetitive action of N on the vector form of the graph states, interspersed with the actions of certain matrices from D. We will show, once more, that these repeated actions not only generate the LC orbit of the graph, but also, simultaneously, generate a subset of the $\{I, H, N\}^n$ transform spectra. It therefore follows that the LC orbit can be identified with a subset of the flat transform spectra of the $\{I, H, N\}^n$ transform set. Consider the action of Non qubit v of a graph G, where N is the 2×2 Negahadamard transform of one qubit. To be more precise, let $s = (-1)^{p(\mathbf{x})}$be the bipolar (± 1) vector where $p(\mathbf{x}) = p(x_0, x_1, \ldots, x_{n-1})$ is a boolean homogeneous quadratic function, such that the existence of $x_j x_k$ in $p(\mathbf{x})$ indicates an edge between vertices j and k in the graph, G. Then the action of N_v on G can be computed as the matrix-vector product, $U_v s$, where:

$$U_v = I \otimes \cdots \otimes I \otimes N \otimes I \otimes \cdots \otimes I$$

where the N matrix occurs at position v in the tensor product decomposition of U_v. We wish to find out how U_v modifies $p(\mathbf{x})$. Let us write $p(\mathbf{x})$, uniquely, as,

$$p(\mathbf{x}) = x_v \mathcal{N}_v(\mathbf{x}) + q(\mathbf{x})$$

where $q(\mathbf{x})$ and $\mathcal{N}_v(\mathbf{x})$ are independent of x_v (note that $\mathcal{N}_v(\mathbf{x})$ has nothing to do with the Negahadamard kernel, N_v). We shall state a theorem that holds for $p(\mathbf{x})$ of any degree, not just quadratic, and then show that it's specialisation to quadratic $p(\mathbf{x})$ gives the required single LC operation. Let us express $\mathcal{N}_v(\mathbf{x})$ as the sum of $r$monomials, $m_i(\mathbf{x})$, as follows,

$$\mathcal{N}_v(\mathbf{x}) = \sum_{i=0}^{r-1} m_i(\mathbf{x})$$

For $p(\mathbf{x})$ of any degree, the $m_i(\mathbf{x})$ are of degree $\leq n-1$. In the sequel we mix arithmetic, mod 2, and mod 4 so, to clarify the formulas for those equations that mix moduli, anything in square brackets is computed (mod 2). The $\{0, 1\}$ result is then embedded in (mod 4) arithmetic for subsequent operations outside the square brackets. We must also define,

$$\mathcal{N}'_v(\mathbf{x}) = \sum_{i=0}^{r-1} [m_i(\mathbf{x})] \qquad (\text{ mod } 4)$$

We now state and prove the following theorem:

Theorem 5. *Let $s' = U_v s$, where $s = (-1)^{p(\mathbf{x})}$ and $s' = i^{p'(\mathbf{x})}$. Then,*

$$p'(\mathbf{x}) = 2\left[p(\mathbf{x}) + \sum_{j \neq k} m_j(\mathbf{x}) m_k(\mathbf{x})\right] + 3\mathcal{N}'_v(\mathbf{x}) + 3[x_v] \qquad (\textit{ mod } 4) \tag{3}$$

Proof. Assign to $A$and B the evaluation of $p(\mathbf{x})$ at $x_v = 0$ and $x_v = 1$, respectively. Thus,

$$A = p(\mathbf{x})_{x_v=0} = q(\mathbf{x})$$

Similarly,

$$B = p(\mathbf{x})_{x_v=1} = \mathcal{N}_v(\mathbf{x}) + q(\mathbf{x})$$

We also need the following equality between arithmetic mod 2 and arithmetic mod 4.

Lemma 4.

$$\sum_{i=1}^{n}[A_i] \quad (\ mod\ 4) = [\sum_{i=1}^{n} A_i] + 2[\sum_{i\neq j} A_i A_j] \quad (\ mod\ 4) \quad where\ A_i \in \mathbb{Z}_2$$

Now observe the following action of N:

$$\begin{aligned}
\tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} &= w\begin{pmatrix} 1 \\ -i \end{pmatrix} \\
\tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}\begin{pmatrix} -1 \\ 1 \end{pmatrix} &= w\begin{pmatrix} i \\ -1 \end{pmatrix} \\
\tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}\begin{pmatrix} 1 \\ -1 \end{pmatrix} &= w\begin{pmatrix} -i \\ 1 \end{pmatrix} \\
\tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}\begin{pmatrix} -1 \\ -1 \end{pmatrix} &= w\begin{pmatrix} -1 \\ i \end{pmatrix}
\end{aligned}$$

where $w = e^{2\pi i/8}$. We can ignore the global constant, w, so that N maps $(-1)^{00}$ to i^{03}, $(-1)^{10}$ to i^{12}, $(-1)^{01}$to $i^{30}$and $(-1)^{11}$ to i^{21}. In general, for $A, B \in \mathbb{Z}_2$, $\alpha, \beta \in \mathbb{Z}_4$, $(-1)^{AB}$ is mapped by N_v to $i^{\alpha\beta}$, where,

$$\begin{aligned}
\alpha &= 2[AB] + [A] + 3[B] \quad (\text{ mod } 4) \\
\beta &= 2[AB] + 3[A] + [B] + 3 \quad (\text{ mod } 4)
\end{aligned}$$

Substituting the previous expressions for A and B into the above equation and making use of Lemma 4 gives us,

$$\begin{aligned}
\alpha(\mathbf{x}) &= 2[q(\mathbf{x})] + 3[\mathcal{N}_v(\mathbf{x})] \quad (\text{ mod } 4) \\
\beta(\mathbf{x}) &= 2[q(\mathbf{x})] + [\mathcal{N}_v(\mathbf{x})] + 3 \quad (\text{ mod } 4)
\end{aligned}$$

The function $p'(\mathbf{x})$ can now be written as,

$$p'(\mathbf{x}) = (3[x_v] + 1)\alpha(\mathbf{x}) + [x_v]\beta(\mathbf{x}) \quad (\text{ mod } 4)$$

Substituting in the expressions for α and β gives,

$$p'(\mathbf{x}) = 2[q(\mathbf{x})] + 2[x_v\mathcal{N}_v(\mathbf{x})] + 3[\mathcal{N}_v(\mathbf{x})] + 3[x_v] \quad (\text{ mod } 4)$$

Applying Lemma 4 to the term $3[\mathcal{N}_v(\mathbf{x})]$,

$$3[\mathcal{N}_v(\mathbf{x})] = 2\left[\sum_{j\neq k} m_j(\mathbf{x})m_k(\mathbf{x})\right] + 3\mathcal{N}'_v(\mathbf{x}) \quad (\text{ mod } 4)$$

Furthermore, Lemma 4 implies that,

$$2\left[\sum_{i=1}^{n} A_i\right](\text{ mod } 4) = 2\sum_{i=1}^{n}[A_i](\text{ mod } 4) \quad \text{where } A_i \in \mathbb{Z}_2$$

□

For $p(\mathbf{x})$a quadratic function, $\mathcal{N}_v(\mathbf{x})$has degree one. This implies that $\mathcal{N}'_v(\mathbf{x})$ is a sum of degree-one terms over $\mathbb{Z}_4$. Therefore the $\mathbb{Z}_4$ degree-one terms, $\mathcal{N}'_v(\mathbf{x})$ and $3[x_v]$ can be eliminated from (3) by appropriate subsequent action by the tensor

product of certain members of the diagonal/anti-diagonal set $\mathbf{D}$. Moreover, as all monomials, $m_i(\mathbf{x})$, are then of degree one, (3) reduces to,

$$p'(\mathbf{x}) \simeq p(\mathbf{x}) + \sum_{j,k \in \mathcal{N}_v, j \neq k} x_j x_k \qquad (\bmod 2) \tag{4}$$

(4) precisely defines the action of a single LC operation at vertex v on the graph form, G, as the "Local Complement" centred at vertex v. As $p'(\mathbf{x})$ is also a quadratic boolean function, we can realise successive LC operations on chosen vertices in G via successive actions of N on the associated chosen positions within the tensor product transform, where each action of N must be interspersed with the tensor product of certain actions from $\mathbf{D}$which eliminate the $\mathbb{Z}_4$-linear terms from (3). In particular, one needs to intersperse with tensor products of $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right)$.

Theorem 6. *Given a graph, G, as represented by $s = (-1)^{p(\mathbf{x})}$, with $p(\mathbf{x})$ quadratic, the LC orbit of G comprises graphs which occur as a subset of the spectra with respect to the action of transforms from $\{I, H, N\}^n$ acting on s.*

Proof. Define $D_1 \subset D$ such that

$$D_1 = \{\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & a \\ b & 0 \end{smallmatrix}\right) \quad | \quad a = 1, b = \pm 1\}.$$

Similarly, define $D_2 \subset D$ such that

$$D_2 = \{\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & a \\ b & 0 \end{smallmatrix}\right) \quad | \quad a = 1, b = \pm i\}, \quad \text{where } i^2 = -1.$$

Then, by computation, it is straightforward to establish that, for any $\Delta_1, \Delta_1' \in D_1$, any $\Delta_2, \Delta_2' \in D_2$, and any $c \in \{1, i, -1, -i\}$,

$$\begin{array}{ll} N\Delta_1 = c\Delta_1' N & H\Delta_1 = c\Delta_1' H \\ N\Delta_2 = c\Delta_1 H & H\Delta_2 = c\Delta_1 N \end{array} \tag{5}$$

Let $\Delta_* \in D_1 \bigcup D_2$. Then, for a given variable x_v (vertex v), succesive applications of $\Delta_* N$ can, using (5), be re-expressed as,

$$\prod(\Delta_* N) = c\Delta_* \prod N \simeq \prod N$$

But, from (2), successive powers of N generate I, H, or N, to within a final multiplication by a member of D. It follows that successive LC actions on arbitrary vertices can be described by the action on s of a member of the transform set, $\{I, H, N\}^n$, and therefore that the LC orbit occurs within the $\{I, H, N\}^n$ transform spectra of s. □

4.4 LC on Hypergraphs

In general, for $p(\mathbf{x})$ of degree > 2, $\mathcal{N}_v(\mathbf{x})$ will typically have degree higher than 1, and therefore the expansion of the sum will contribute higher degree terms. For such a scenario we can no longer eliminate the nonlinear and non-boolean term, $\mathcal{N}_v'(\mathbf{x})$, from the right-hand side of (3) by subsequent actions from $\mathbf{D}$. Therefore, it is typically not possible to iterate LC graphically beyond one step. We would like to identify hypergraph equivalence wrt local unitary transforms, in particular wrt $\{I, H, N\}^n$. Computations have shown that orbits of boolean functions of degree > 2 and size greater than one do sometimes exist with respect to $\{I, H, N\}^n$, although they appear to be significantly smaller in size compared to the orbits for the quadratic case [17].

An interesting open problem is to characterise a 'LC-like' equivalence for hypergraphs.

4.5 Further Spectral Symmetries of Boolean Functions with respect to the $\{I, H, N\}^n$ Spectra

It is well-known that the power spectrum of the Walsh-Hadamard transform of a boolean function is invariant to within a re-ordering of the spectral elements after an invertible affine transformation of the variables of the boolean function [4]. This implies that Bent boolean functions remain Bent after affine transform (see Section 5 for a discussion of Bent properties). However, the set of $\{I, H, N\}^n$ power spectra are not an invariant of affine transformation. We are therefore constrained to a much smaller set of symmetries over which to establish $\{I, H, N\}^n$ power spectral invariance. In this section we ascertain for which binary transformations (other than LC) the power spectra of the $\{I, H, N\}^n$ transform remains invariant to within a re-ordering of the spectral elements within each spectrum. In the sequel we refer to the complete set of $3^n \times 2^n$ power spectral values wrt $\{I, H, N\}^n$ as $\mathbf{S_{IHN}}$. Moreover, by 'invariance' we imply that we allow any re-ordering of the $3^n \times 2^n$ spectral elements.

From the discussion of section 4.1 and lemma 20 it is evident that $\mathbf{S_{IHN}}$ of a quadratic boolean function is invariant after LC transformation. Thus, for instance, if the highest value within $\mathbf{S_{IHN}}$ for a given quadratic boolean function, $p(\mathbf{x})$, has value t, then t is also the highest value within $\mathbf{S_{IHN}}$ for any quadratic boolean function, $p'(\mathbf{x})$, in the same LC orbit as $p(\mathbf{x})$. However the LC orbit is not the only spectral symmetry exhibited with respect to $\mathbf{S_{IHN}}$. We identify the following symmetries. The first is trivial.

Lemma 5. *Let $p(\mathbf{x})$ be a boolean function of* any *degree. Then $\mathbf{S_{IHN}}$ of $p(\mathbf{x})$ and $\mathbf{S_{IHN}}$ of $p(\mathbf{x}) + l(\mathbf{x})$ are equivalent, where l is any affine function of its arguments.*

Lemma 6. *Let $p(\mathbf{x})$ be a boolean function of* any *degree over n variables. Then $\mathbf{S_{IHN}}$ of $p(\mathbf{x})$ and $\mathbf{S_{IHN}}$ of $p(\mathbf{x} + \mathbf{a})$ are equivalent, where $\mathbf{a} \in \mathbb{Z}_2^n$.*

Proof. Replacing x_j with $x_j + 1$ within any $p(\mathbf{x})$ is equivalent to the action of the 'bit-flip' operator, $\sigma_x = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, at index j of $(-1)^{p(\mathbf{x})}$.

We can rewrite $H\sigma_x$ as follows,

$$H\sigma_x = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) H = \sigma_z H$$

In other words, a bit-flip (or periodic shift) followed by the action of H is identical to the action of H followed by a 'phase-flip'. (This is well-known to quantum code theorists). The final phase-flip is a member of the set $\mathbf{D}$ so does not change the magnitude of the spectral values produced by H. Therefore the power spectra produced by H is invariant to a prior periodic shift.

Similarly, we can rewrite $N\sigma_x$as follows,

$$N\sigma_x = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & i \\ 1 & -i \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 0 & i \\ -i & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & i \\ 1 & -i \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & i \\ -i & 0 \end{smallmatrix}\right) N = -\sigma_y N$$

where σ_y is one of the four Pauli matrices. In other words, a bit-flip (or periodic shift) followed by the action of N is identical to the action of N followed by a member of the set $\mathbf{D}$. Therefore the power spectra produced by N is invariant to a prior periodic shift. (Note that (5) also leads us to the same conclusion).

The above argument is trivial with respect to the I matrix, $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Moreover, the argument is naturally extended to any n-dimensional tensor product of I, H, and N. □

[4] The power of the kth spectral element, S_k, is given by $|S_k|^2$.

We summarise all symmetries generated by affine offset and by periodic shift as follows:

Let $p(\mathbf{x})$ be a boolean function of *any* degree over n variables. We perform a combination of affine offset and periodic shift on $p(\mathbf{x})$ by the following operation:

$$p(\mathbf{x}) \Rightarrow p(\mathbf{x}+\mathbf{a}) + \mathbf{c}\cdot\mathbf{x} + d$$

where $\mathbf{a}, \mathbf{c} \in \mathbb{Z}_2^n$, $d \in \mathbb{Z}_2$, and '$\cdot$' is the scalar product.

The symmetries generated by affine offset and by periodic shift comprise all symmetries generated by any combination of periodic and negaperiodic shift, because we perform a combination of periodic and negaperiodic shifts on $p(\mathbf{x})$ by the following operation:

$$p(\mathbf{x}) \Rightarrow p(\mathbf{x}+\mathbf{a}) + \mathbf{c}\cdot\mathbf{x} + \ \mathrm{wt}(\mathbf{c}), \qquad \mathbf{c} \preceq \mathbf{a}$$

where $\mathbf{a}, \mathbf{c} \in \mathbb{Z}_2^n$, '$\mathbf{c} \preceq \mathbf{a}$' means that $c_i \leq a_i$, $\forall i$ (i.e. *a covers c*), $d \in \mathbb{Z}_2$, '$\cdot$' is the scalar dot product, and $\mathrm{wt}(\mathbf{c})$ means the binary weight of $\mathbf{c}$. The one positions in $\mathbf{a}$ identify the variables x_i which are to undergo periodic or negaperiodic shift, and the one positions in $\mathbf{c}$ identify the variables x_i which are to undergo negaperiodic shift. The combined periodic and negaperiodic symmetry induced by $\{I, H, N\}$ implies an aperiodic symmetry, as discussed further in [17].

5 Generalised Bent Properties of Boolean Functions

5.1 Bent Boolean Functions

A Bent boolean function can be defined by means of the WHT. Let $p(\mathbf{x})$ be our function over $n$binary variables, as before. Define the WHT of $p(\mathbf{x})$ by,

$$P_{\mathbf{k}} = 2^{-n/2} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{p(\mathbf{x})+\mathbf{k}\cdot\mathbf{x}} \tag{6}$$

where $\mathbf{x}, \mathbf{k} \in \mathbb{Z}_2^n$, and $\cdot$ implies the scalar product of vectors.

The WHT of $p(\mathbf{x})$ can alternatively be defined as a multiplication of the vector $(-1)^{p(\mathbf{x})}$ by $H \otimes H \otimes \ldots \otimes H$. Thus,

$$P = 2^{-n/2}(H \otimes H \otimes \ldots \otimes H)(-1)^{p(\mathbf{x})} = 2^{-n/2}(\bigotimes_{i=0}^{n-1} H)(-1)^{p(\mathbf{x})} \tag{7}$$

where $P \in \mathcal{C}^{2^n}$.
$p(\mathbf{x})$ is defined to be *Bent* if $|P_{\mathbf{k}}| = 1\ \forall \mathbf{k}$, in which case we say that $p(\mathbf{x})$ has a *flat* spectra wrt the WHT. In other words, $p(\mathbf{x})$ is Bent if P is *flat*.

Let Γ be an $n \times n$ binary adjacency matrix associated to $p(\mathbf{x})$ for the case when $p(\mathbf{x})$ is a quadratic, such that, if $p(\mathbf{x}) = \sum_{(j,k)\in\mathbf{E}} x_j x_k + \mathbf{c}\cdot\mathbf{x} + d$, where $\mathbf{c} \in \mathbb{Z}_2^n$, $d \in \mathbb{Z}_2$, and $\mathbf{E}$is the associated edge set with $k > j$, then $\Gamma_{j,k} = \Gamma_{k,j} = 1$ for $(j,k) \in \mathbf{E}$ and $\Gamma_{j,k} = 0$, otherwise. Then an alternative way to define the Bent property of $p(\mathbf{x})$ when $p(\mathbf{x})$ is a quadratic is as follows.

Lemma 7. *[30]*

$$p(\mathbf{x})\ \textit{is Bent} \quad \Leftrightarrow \quad \Gamma\ \textit{has maximum rank, mod 2}$$

It is well-known [30] that all Bent quadratics are affine equivalent to the boolean function $\left(\sum_{i=0}^{\frac{n}{2}-1} x_{2i}x_{2i+1}\right) + \mathbf{c}\cdot\mathbf{x} + d$ for n even, only, where $\mathbf{c} \in \mathbb{Z}_2^n$, and $d \in \mathbb{Z}_2$. More generally, Bent boolean functions only exist for n even. However, for n even, not all boolean quadratic functions are Bent. For instance, $x_0x_1 + x_0x_2 + x_0x_3$ is not a Bent boolean function. It is interesting to investigate other Bent symmetries where affine symmetry has been omitted. In particular, in the context of LC, we are interested in the existence and number of flat spectra of boolean functions with respect to the $\{H,N\}^n$-transform set ($Bent_4$), the $\{I,H\}^n$-transform set ($IBent$), and the $\{I,H,N\}^n$-transform set ($IBent_4$). In the following subsections we investigate the Bent_4, $\mathbb{Z}_4$-Bent, (Completely) IBent, LC-Bent, and (Completely) IBent_4 properties of connected quadratic boolean functions, where affine symmetry is omitted, and make some general statements about these properties for more general boolean functions. As mentioned in the introduction, some recent papers [2, 1, 4, 5] have proposed *interlace polynomials* to describe interlace/circle graphs. In particular $q(x)$ and $Q(x)$ are defined, these being certain *Martin polynomials*, as proposed by Bouchet [10]. It can be shown that $q(x)$ and $Q(x)$ summarise certain aspects of the spectra of a graph wrt $\{I,H\}^n$ and $\{I,H,N\}^n$, respectively. In particular, $q(1)$ and $Q(2)$ evaluate the number of flat spectra wrt $\{I,H\}^n$ and $\{I,H,N\}^n$, respectively.

5.2 Bent Properties with respect to the $\{H,N\}^n$-Transform Set

We now investigate certain spectral properties of the boolean functions wrt the $\{H,N\}^n$ transform set, where $\{H,N\}^n$ is the set of 2^n transforms of the form $\bigotimes_{i=0}^{n-1}\{H,N\}$.

5.2.1 All Graph States are Bent_4

The following is trivial to verify for a boolean function, $p(\mathbf{x})$:

$$p(\mathbf{x}) \text{ is Bent } \Leftrightarrow p(\mathbf{x}) + \mathbf{k}\cdot\mathbf{x} + d \qquad \text{is Bent}$$

where $\mathbf{k} \in \mathbb{Z}_2^n$ and $d \in \mathbb{Z}_2$. In other words, if $p(\mathbf{x})$ is Bent then so are all its affine offsets, mod 2. However the above does not follow if one considers every possible $\mathbb{Z}_4$-linear offset of the boolean function. The WHT of a function from $\mathbb{Z}_2^n$to $\mathbb{Z}_2$ (a boolean function) with a $\mathbb{Z}_4$-linear offset can be defined as follows.

$$P_{\mathbf{k},\mathbf{c}} = 2^{-n/2}\sum_{\mathbf{x}\in\mathbb{Z}_2^n} (i)^{2[p(\mathbf{x})+\mathbf{k}\cdot\mathbf{x}]+\mathbf{c}\cdot\mathbf{x}} \qquad \mathbf{k},\mathbf{c} \in \mathbb{Z}_2^n \tag{8}$$

Given (8) we define a boolean function as Bent_4 as follows.

Definition 4.

$$p(\mathbf{x}) \textit{ is } Bent_4 \quad \Leftrightarrow \quad \exists \mathbf{c} \textit{ such that } |P_{\mathbf{k},\mathbf{c}}| = 1 \qquad \forall \mathbf{k} \in \mathbb{Z}_2^n$$

Let $\mathbf{R_N}$and $\mathbf{R_H}$ be integer sets that partition $\{0,1,\ldots,n-1\}$. Let,

$$U = \bigotimes_{j\in\mathbf{R_H}} H_j \bigotimes_{j\in\mathbf{R_N}} N_j$$

Let,

$$s' = U(-1)^{p(\mathbf{x})} \tag{9}$$

Lemma 8. *$p(\mathbf{x})$ is Bent$_4$ if $\exists$one or more partitions, $\mathbf{R_N}, \mathbf{R_H}$ such that $s'$is* flat.

Proof. The rows of Ucan be described by $(i)^{f(\mathbf{x})}$, where $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$, where $f$is linear, $f : \mathbb{Z}_2^n \to \mathbb{Z}_4$, and the coefficient of x_j in f is $\in \{0, 2\}$ for $j \in \mathbf{R_H}$ and $\in \{1, 3\}$for $j \in \mathbf{R_N}$. Therefore s'can always, equivalently, be expressed as $s' = (\bigotimes H)(i)^{2p[\mathbf{x}]+[f'(\mathbf{x})]}$where f' is linear, $f' : \mathbb{Z}_2^n \to \mathbb{Z}_2$, and the coefficient of x_j in f' is 0 for $j \in \mathbf{R_H}$, and 1 for $j \in \mathbf{R_N}$. □

An alternative way to define the Bent$_4$ property of $p(\mathbf{x})$, when $p(\mathbf{x})$ is a quadratic boolean function of n variables, is via a modified form of the adjacency matrix.

Lemma 9. *For quadratic $p(\mathbf{x})$,*

$$p(\mathbf{x}) \text{ is Bent}_4 \quad \Leftrightarrow \quad \Gamma + diag(v) \text{ has maximum rank, mod 2,} \quad \text{where } v \in \mathbb{Z}_2^n$$

for one or more choices of v.

Proof. We first show that the transform of $(-1)^{p(\mathbf{x})}$ by tensor products of $H$and N produces a flat spectra if and only if the associated periodic and negaperiodic autocorrelation spectra have zero out-of-phase values. We then show how these autocorrelation constraints lead directly to constraints on the associated adjacency matrix.

Consider functions, p, of just one variable, x_0, and let $s = (-1)^{p(x_0)}$. Define the periodic autocorrelation function as follows,

$$a_k = \sum_{x_0 \in \mathbb{Z}_2} (-1)^{p(x_0)+p(x_0+k)}, \qquad k \in \mathbb{Z}_2$$

Then it is well-known that $s' = Hs$ is a flat spectrum if and only if $a_k = 0$ for $k \neq 0$.

Define the negaperiodic autocorrelation function as follows,

$$b_k = \sum_{x_0 \in \mathbb{Z}_2} (-1)^{p(x_0)+p(x_0+k)+x_0+1}, \qquad k \in \mathbb{Z}_2$$

Then it is similarly true that $s' = Ns$ is a flat spectrum if and only if $b_k = 0$ for $k \neq 0$. (In fact, for p a boolean function of just one variable, Hs is never flat and Ns is always flat, but this is a special case that only holds for one variable).

We now elaborate on the above two claims. Define $s(z) = s_0 + s_1 z$, $a(z) = a_0 + a_1 z$, and $b(z) = b_0 + b_1 z$. Then the periodic and negaperiodic relationships between autocorrelation and fourier spectra, as claimed above, follow because periodic autocorrelation can be realised by the polynomial multiplication, $a(z) = s(z)s(z^{-1})$ mod $(z^2 - 1)$, with associated residue reduction, mod $(z - 1)$ and mod $(z + 1)$, realised by $s' = Hs = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} s$, (with the Chinese Remainder Theorem realised by $H^\dagger s'$, where '$\dagger$' means transpose conjugate). By Parseval, s' can only be flat if $a_1 = 0$. Similarly, negaperiodic autocorrelation can be realised by the polynomial multiplication, $b(z) = s(z)s(z^{-1})$ mod $(z^2 + 1)$, with associated residue reduction, mod $(z - i)$ and mod $(z + i)$, realised by $s' = Ns = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} s$, (with the Chinese Remainder Theorem realised by $N^\dagger s'$). By Parseval, s' can only be flat if $b_1 = 0$.

We can simply extend this autocorrelation$\leftrightarrow$Fourier spectrum duality to n binary variables by defining multivariate forms of the above polynomial relationships.

Thus, if we choose periodic autocorrelation for indices in $\mathbf{R_H}$ and negaperiodic autocorrelation for indices in $\mathbf{R_N}$, we obtain the autocorrelation spectra,

$$A_{\mathbf{k},\mathbf{R_H},\mathbf{R_N}} = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{p(\mathbf{x})+p(\mathbf{x}+\mathbf{k})+\sum_{i=1}^{n-1}\chi_{\mathbf{R_N}}(i)k_i x_i+\sum_{i=1}^{n-1}\chi_{\mathbf{R_N}}(i)k_i},$$

where $\mathbf{k} = (k_0, k_1, \ldots, k_{n-1}) \in \mathbb{Z}_2^n$, and $\chi_{\mathbf{R_N}}(i)$ is the characteristic function of $\mathbf{R_N}$, i.e, $\chi_{\mathbf{R_N}}(i) = 1\ \forall i \in \mathbf{R_N}$, $\chi_{\mathbf{R_N}}(i) = 0\ \forall i \notin \mathbf{R_N}$. In polynomial terms, with $\mathbf{z} \in \mathbb{Z}_2^n$ and $s(\mathbf{z}) = \sum_{\mathbf{j}\in\mathbb{Z}_2^n} s_{\mathbf{j}} \prod_{i\in\mathbb{Z}_n} z_i^{j_i}$, we have,

$$\begin{aligned} A_{\mathbf{R_H},\mathbf{R_N}}(\mathbf{z}) &= \textstyle\sum_{\mathbf{k}\in\mathbb{Z}_2^n} A_{\mathbf{k},\mathbf{R_H},\mathbf{R_N}} \prod_{i\in\mathbb{Z}_n} z_i^{k_i} \\ &= s(z_0, z_1, \ldots, z_{n-1}) s(z_0^{-1}, z_1^{-1}, \ldots, z_{n-1}^{-1}) \bmod \textstyle\prod_{i\in\mathbb{Z}_n}(z_i^2 - (-1)^{\chi_{\mathbf{R_N}}(i)}) \end{aligned} \tag{10}$$

Then, by appealing to a multivariate version of Parseval's Theorem, s' as defined in (9) is flat if and only if $A_{\mathbf{k},\mathbf{R_H},\mathbf{R_N}} = 0$, $\forall \mathbf{k}$, $\mathbf{k} \neq \mathbf{0}$.

These constraints on the autocorrelation coefficients of s translate to requiring a maximum rank property for a modified adjacency matrix, as follows. The condition $A_{\mathbf{k},\mathbf{R_H},\mathbf{R_N}} = 0$ for $\mathbf{k} \neq \mathbf{0}$ is equivalent to requiring that, if we compare the function with its multidimensional periodic and negaperiodic rotations (but for the case of the identity rotation), the remainder should be a balanced function. When dealing with quadratic boolean functions, the remainder is always a linear or constant function, and therefore it will be balanced unless it is a constant function. This gives us a system of linear equations, and the matrix of the system is the binary adjacency matrix, Γ, of $p(\mathbf{x})$, with a modified diagonal, that is with $\Gamma_{i,i} = 1 \forall i \in \mathbf{R_N}$, and $\Gamma_{i,i} = 0$ otherwise. To prove this we consider the algebraic normal form (ANF) of the function:

$$p(x_0, x_1, \ldots, x_{n-1}) = a_{01}x_0x_1 + a_{02}x_0x_2 + \cdots + a_{ij}x_ix_j + \cdots + a_{n-2,n-1}x_{n-2}x_{n-1}$$

This, expressed as the adjacency matrix of the graph, is:

$$\Gamma = \begin{pmatrix} 0 & a_{01} & a_{02} & \cdots & a_{0,n-1} \\ a_{01} & 0 & a_{12} & \cdots & a_{1,n-1} \\ a_{02} & a_{12} & 0 & \cdots & a_{2,n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{0,n-1} & a_{1,n-1} & a_{2,n-1} & \cdots & 0 \end{pmatrix}$$

Substituting in the ANF, we see that

$$\begin{aligned} &p(x_0 + k_0, \ldots, x_{n-1} + k_{n-1}) = p(x_0, \ldots, x_{n-1}) + \\ &k_0(a_{01}x_1 + a_{02}x_2 + \cdots + a_{0,n-1}x_{n-1}) + k_1(a_{01}x_0 + a_{02}x_2 + \cdots + a_{0,n-1}x_{n-1}) + \cdots \\ &+ \cdots + k_{n-1}(a_{0,n-1}x_0 + a_{1,n-1}x_2 + \cdots + a_{n-2,n-1}x_{n-2}) \end{aligned}$$

Therefore,

$$\begin{aligned} &p(\mathbf{x}) + p(\mathbf{x}+\mathbf{k}) + \textstyle\sum_{i=1}^{n-1} \chi_{\mathbf{R_N}}(i)k_ix_i = \\ &k_0(\chi_{\mathbf{R_N}}(0)x_0 + a_{01}x_1 + a_{02}x_2 + \cdots + a_{0,n-1}x_{n-1}) + \\ &+k_1(a_{01}x_0 + \chi_{\mathbf{R_N}}(1)x_1 + a_{02}x_2 + \cdots + a_{0,n-1}x_{n-1}) + \cdots + \\ &+k_{n-1}(a_{0,n-1}x_0 + a_{1,n-1}x_2 + \cdots + a_{n-2,n-1}x_{n-2} + \chi_{\mathbf{R_N}}(n-1)x_{n-1}) = \\ &x_0(\chi_{\mathbf{R_N}}(0)k_0 + a_{01}k_1 + ... + a_{0n}k_n) + x_1(a_{01}k_0 + \chi_{\mathbf{R_N}}(1)k_1 + \cdots a_{1,n-1}k_{n-1}) + \\ &+ \cdots + \cdots + x_{n-1}(a_{0,n-1}k_0 + a_{1,n-1}k_1 + ... + a_{n-2,n-1}k_{n-2} + \chi_{\mathbf{R_N}}(n-1)x_{n-1}) \end{aligned}$$

This, being a linear or constant term, will be balanced unless it is constant, i.e., unless the linear part is zero. The constant factor won't play any role in the equation

$A_{\mathbf{k}} = 0$, and can be thus ignored. We have the the following system of equations:

$$\begin{array}{l}
\chi_{\mathbf{R_N}}(0)k_0 + a_{01}k_1 + a_{02}k_2 + \cdots + a_{0,n-1}k_{n-1} = 0 \\
a_{01}k_0 + \chi_{\mathbf{R_N}}(1)k_1 + a_{12}k_2 + \cdots + a_{1,n-1}k_{n-1} = 0 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
a_{0,n-1}k_0 + a_{1,n-1}k_1 + \cdots + a_{n-2,n-1}k_{n-2} + \chi_{\mathbf{R_N}}(n-1)k_{n-1} = 0
\end{array}$$

Writing this system of linear equations as a matrix, we have:

$$\begin{pmatrix}
\chi_{\mathbf{R_N}}(0) & a_{01} & a_{02} & \cdots & a_{0,n-1} \\
a_{01} & \chi_{\mathbf{R_N}}(1) & a_{12} & \cdots & a_{1,n-1} \\
a_{02} & a_{12} & \chi_{\mathbf{R_N}}(2) & \cdots & a_{2,n-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
a_{0,n-1} & a_{1,n-1} & a_{2,n-1} & \cdots & \chi_{\mathbf{R_N}}(n-1)
\end{pmatrix}$$

This is clearly a modification of the adjacency matrix, with 1 or 0 in the position i of the diagonal depending on if $i \in \mathbf{R_N}$ or $i \in \mathbf{R_H}$, that is, if we apply N or H in the position i. □

In general,

$$p(\mathbf{x}) \text{ is Bent } \begin{array}{c} \Rightarrow \\ \not\Leftarrow \end{array} \quad p(\mathbf{x}) \text{ is Bent}_4$$

We now state and prove the following Theorem.

Theorem 7. *All boolean functions of degree ≤ 2 are Bent$_4$.*

Proof. Degree zero and degree one functions are trivial. Consider the adjacency matrix, Γ, associated with the quadratic boolean function, $p(\mathbf{x})$. Γ has zeroes on the diagonal. We need the following lemma.

Lemma 10. *$\Gamma + diag(v)$ has maximum rank (mod 2) for at least one choice of v, where $v \in \mathbb{Z}_2^n$.*

Proof. Let Γ be the adjacency matrix, and let M be the minor associated with the first entry of the matrix, i.e., let

$$\Gamma = \begin{pmatrix} 0 & \\ & M \end{pmatrix}$$

We want to see that there exists at least one choice of v such that $\Gamma + \mathrm{diag}(v)$ has maximum rank (mod 2). We prove it by induction on the number of variables of the function:

Trivially, the lemma is true for $n = 2$: in this case,

$$\Gamma = \begin{pmatrix} 0 & a \\ a & 0 \end{pmatrix}$$

Then, either $\det(\Gamma) = 1$, in which case we just choose $v = (0, 0)$, or $a = 0$ (empty graph). In the last case we can change both entries of the diagonal, choosing $v = (1, 1)$, and then $det(\Gamma + \mathrm{diag}(v)) = 1 + a = 1$. Suppose now that the lemma is true for $n - 1$ variables. We'll see that it is true for n variables. Let Γ be the

adjacency matrix of a quadratic boolean function in n variables, and consider its determinant (always mod 2). If the determinant of Γ is 1, we take $v = (0, ..., 0)$, and we're done. Suppose that $\det(\Gamma) = 0(\bmod 2)$. Then we look at the determinant of M. We have two cases:

- $\det(M) = 1$: we take $v = (1, 0, ..., 0)$, that is,

$$\Gamma + \mathrm{diag}(v) = \begin{pmatrix} 1 & \\ & M \end{pmatrix}$$

- $det(M) = 0$: By the hypothesis of induction, there is at least one choice of $v(M) \in \mathbb{Z}_2^{n-1}$, $v(M) = (v_1, ..., v_{n-1})$ such that $M + \mathrm{diag}(v_M)$ has full rank. We take $v' = (0, v_1, ..., v_{n-1}) \in \mathbb{Z}_2^n$, and compute the determinant of $\Gamma + \mathrm{diag}(v')$. If it is one, we've finished. If it's zero, we are in the first case again, so we just take $v = (1, v_1, ..., v_{n-1})$, and we're done.

□

The Theorem follows by considering Lemmas 9 and 10. □

Obs.: Lemma 10 and Theorem 7 are true even for boolean functions associated with non-connected (or even empty) graphs.

5.2.2 Not All Boolean Functions are Bent$_4$

Lemma 11. *Not all boolean functions of degree > 2 are Bent$_4$.*

Proof. By counter-example. For instance, by computation there are no Bent$_4$ cubics of three variables. □

Further computations show that there are no Bent$_4$ boolean functions of four variables of degree > 2. Similarly, by computation, there are only 252336 Bent$_4$ cubic boolean functions in five variables (out of a possible $2^{20} - 2^{10}$, not including affine offsets), and no Bent$_4$ boolean functions of degree ≥ 4 in five variables. Bent$_4$ cubics of six variables do exist. Lemma 11 raises an interesting question which we leave as an open problem:

What is the maximum algebraic degree of a Bent$_4$ boolean function of n variables?

5.2.3 There are No $\mathbb{Z}_4$-Bent Boolean Functions

A very strict spectral criteria is the $\mathbb{Z}_4$-Bent criteria. Given (8) we define a boolean function as $\mathbb{Z}_4$-Bent as follows.

Definition 5.

$$p(\mathbf{x}) \text{ is } \mathbb{Z}_4\text{-Bent} \Leftrightarrow |P_{\mathbf{k},\mathbf{c}}| = 1 \qquad \forall \mathbf{c}, \mathbf{k} \in \mathbb{Z}_2^n$$

The definition requires that **all** $\mathbb{Z}_4$-linear offsets of the boolean function, $p(\mathbf{x})$, are flat wrt the WHT. It is not expected that such boolean functions exist at all and we now prove this to be the case, first for all boolean functions of degree ≤ 2, and then for all boolean functions.

Theorem 8. *There are no $\mathbb{Z}_4$-Bent quadratic boolean functions.*

Proof. This is trivial for degree zero and degree one functions.

Consider the adjacency matrix, Γ, associated with the quadratic boolean function, $p(\mathbf{x})$. The theorem is equivalent to proving that there is a v such that $\Gamma + \mathrm{diag}(v)$ has rank less than maximal. Then:

- 1) if the functions are non-bent, then we take $v = (0, ..., 0)$ and we're done
- 2) if the function is bent, we take M as in Lemma 7. Now, if $det(M) = 1$, we take $v = (1, 0, ..., 0)$ and we're done; if $det(M) = 0$, we can change it by Lemma 7. Now we look at the determinant of the new matrix. If it's 0, we're done; if not, we are in case 1).

□

We now give a theorem that generalises the above to boolean functions of any degree.

Theorem 9. *There are no $\mathbb{Z}_4$-Bent boolean functions.*

Proof. Consider, once again, the proof of Lemma 9. We have already used Parseval to establish that, for a fixed choice of $\mathbf{R_H}$ and $\mathbf{R_N}$, s', as defined in (9), is flat if and only if $A_{\mathbf{k},\mathbf{R_H},\mathbf{R_N}} = 0$, $\forall \mathbf{k}$, $\mathbf{k} \neq \mathbf{0}$. Therefore $p(\mathbf{x})$ is $\mathbb{Z}_4$-Bent iff $A_{\mathbf{k},\mathbf{R_H},\mathbf{R_N}} = 0$, $\forall \mathbf{k}$, $\mathbf{k} \neq \mathbf{0}$, for **all** bipartite splittings, $\mathbf{R_H}$ and $\mathbf{R_N}$. In particular, if $p(\mathbf{x})$ is $\mathbb{Z}_4$-Bent, then the residue polynomials, $A_{\mathbf{R_H},\mathbf{R_N}}(\mathbf{z})$, as defined in (10), satisfy $A_{\mathbf{R_H},\mathbf{R_N}}(\mathbf{z}) = 2^n$ for all choices of $\mathbf{R_H}$ and $\mathbf{R_N}$ (i.e. their out-of-phase coefficients are all zero). By the Chinese Remainder Theorem (CRT) we can combine these residue polynomials for each choice of $\mathbf{R_H}$ and $\mathbf{R_N}$ to construct the polynomial,

$$r(\mathbf{z}) \bmod \prod_{j \in \mathbb{Z}_n} (z_j^4 - 1) = \mathrm{CRT}\{A_{\mathbf{R_H},\mathbf{R_N}}(\mathbf{z}) \quad | \quad \forall \mathbf{R_H}, \mathbf{R_N}\} \qquad (11)$$

where $r(\mathbf{z}) = s(z_0, z_1, \ldots, z_{n-1}) s(z_0^{-1}, z_1^{-1}, \ldots, z_{n-1}^{-1})$.

But as $r(\mathbf{z})$has an effective degree of two or less over each variable, z_i, the modular restriction in (11) has no effect and, therefore,

$$r(\mathbf{z}) \equiv r(\mathbf{z}) \bmod \prod_{j \in \mathbb{Z}_n} (z_j^4 - 1)$$

It follows, by application of the CRT to (11) that, if $A_{\mathbf{R_H},\mathbf{R_N}}(\mathbf{z}) = 2^n$, $\forall \mathbf{R_H}, \mathbf{R_N}$, then $r(\mathbf{z}) = 2^n$ also, i.e. $r(\mathbf{z})$ is integer. But this is impossible as the coefficients of the maximum degree terms, $\prod_j z_j^{-1^{u_j}}$, $u_j \in \mathbb{Z}_2$, in $r(\mathbf{z})$can never be zero, but are always ± 1. Therefore $p(\mathbf{x})$ can never be $\mathbb{Z}_4$-Bent. □

Remark: Although the proof above was given for boolean functions, it is possible to generalise the proof so as to state that no function from $\mathbb{Z}_2 \to \mathbb{Z}_q$ can be $\mathbb{Z}_4$-Bent, for any even integer q, by embedding $r(\mathbf{z})$ in $r(\mathbf{z}) \bmod \prod_{j \in \mathbb{Z}_n} (z_j^4 - \alpha)$, where α is a 2^tth complex root of 1, $t \to \infty$.

5.2.4 On the Number of Flat Spectra of Quadratic Boolean Functions with respect to $\{H, N\}^n$

It is of interest to construct boolean functions such that a largest subset of the 2^n $\{H, N\}^n$ spectra are flat. The multivariate complementary set constructions of [36] provide candidate functions. The simplest and strongest of these is the *line function* (or *path graph*) [39, 24, 19]. The *line function*, $p_l(\mathbf{x})$ is defined as,

$$p_l(\mathbf{x}) = \sum_{j=0}^{n-2} x_j x_{j+1} + \mathbf{c} \cdot \mathbf{x} + d \tag{12}$$

where $\mathbf{c} \in \mathbb{Z}_2^n$, $d \in \mathbb{Z}_2$, for which the number of flat spectra with respect to $\{H, N\}^n$ is as follows.

Lemma 12. *$K_n = \#$ flat spectra$(p_l(\mathbf{x}))$ wrt $\{H, N\}^n = 2^n - K_{n-1}$; in closed form,*

$$K_n = \frac{1}{3}\left(2^{n+1} + (-1)^n\right)$$

Proof. The modified matrix of the line, $\Gamma +$ diag(v), is as follows:

$$\Gamma = \begin{pmatrix} v_0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & v_1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & v_2 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & 1 & v_{n-1} \end{pmatrix}$$

Solving the determinant by minors, we get the recursion formula

$$D_n = v_0 D_{n-1} + D_{n-2}$$

where D_{n-j} is the determinant of the modified matrix of the line in the variables $x_j, \dots, x_{n-1}$. The spectra will be flat iff $D_n = 1$. In order to get this, we consider the following cases:

1. $D_{n-1} = 0, D_{n-2} = 1$. Then, v_0 can be 0 or 1.
2. $D_{n-1} = 1, D_{n-2} = 1$. Then, $v_0 = 0$.
3. $D_{n-1} = 1, D_{n-2} = 0$. Then, $v_0 = 1$.

We have then $K_n = 2N1 + N2 + N3$, where Ni is the number of times the ith case is true. Note that $\{v_1, \dots, v_{n-1} | D_{n-1}, D_{n-2} = 1\} \cup \{v_1, \dots, v_{n-1} | D_{n-1} = 1, D_{n-2} = 0\} = \{v_1, \dots, v_{n-1} | D_{n-1} = 1\}$, and therefore $N2 + N3 = K_{n-1}$.

We see now that $\{v_1, \dots, v_{n-1} | D_{n-1} = 0, D_{n-2} = 1\} = \{v_1, \dots, v_{n-1}|$ $D_{n-1} = 0\}$, and so $N1 = 2^{n-1} - K_{n-1}$. Suppose $D_{n-1} = D_{n-2} = 0$, As $D_{n-1} = v_1 D_{n-2} + D_{n-3}$, this implies $D_{n-3} = 0$. By the same argument, we must have $D_i = 0,\ 1 \le i \le n-1$. However, if $D_1 = v_{n-1} = 0$ then $D_2 = v_{n-2} v_{n-1} + 1 = 1$, and this leads to a contradiction.

Finally, $K_n = 2(2^{n-1} - K_{n-1}) + K_{n-1} = 2^n - K_{n-1}$. Expanding this recurrence relation, and as $N_0 = 1$, we get $K_n = \sum_{k=0}^{n} (-1)^{n+k} 2^k = \frac{1}{3}\left(2^{n+1} + (-1)^n\right)$. □

For the *clique function* (i.e. the *complete graph*),

$$p_c(\mathbf{x}) = \sum_{i<j} x_i x_j \tag{13}$$

the number of flat spectra with respect to $\{H, N\}^n$ is as follows.

Lemma 13. *K_n = # flat spectra$(p_c(\mathbf{x}))$ wrt $\{H, N\}^n = K_{n-1} + 1 + (-1)^n$; in closed form,*

$$K_n = n + \frac{1 + (-1)^n}{2}$$

Proof. The modified adjacency matrix of the clique is as follows:

$$\Gamma_N = \begin{pmatrix} v_0 & 1 & 1 & 1 & \dots & 1 \\ 1 & v_1 & 1 & 1 & \dots & 1 \\ 1 & 1 & v_2 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & 1 & \dots & v_{n-1} \end{pmatrix}$$

Applying N in the position i to the bipolar vector of the clique is equivalent to making $v_i = 1$. If two or more of the v_i's are 1, then the matrix won't have full rank, so $|\mathbf{R_N}| \leq 1$.

Suppose $|\mathbf{R_N}| = 1$. Solving the determinant by minors, we get $D = \det(\Gamma_N) = \det(\Gamma) + m$, where m is the minor corresponding to v_i. Obviously, m is the determinant of the adjacency matrix of a clique in $n-1$ variables. It is known that the clique in n variables is bent iff n is even. So, if n is even, we have $\det(\Gamma) = 1$, $m = 0$, and so $D = 1$. On the other hand, if n is odd, we have $\det(\Gamma) = 0$, $m = 1$, and so $D = 1$. This means that for every position in which we choose to apply N we have a flat spectra, and therefore we get n flat spectra for this case.

Suppose $|\mathbf{R_N}| = 0$. We know that the clique is bent in an even number of variables, so we have flat spectra iff n is even.

From the preceding argument, we see that $K_n = n + \frac{1+(-1)^n}{2}$. The recurrence form follows trivially. □

By combining the clique and line graphs in certain ways we can get an improvement in the number of flat spectra wrt the clique, but we are still far from the number of flat spectra of the line. Specifically, for the *clique-line-clique*,

$$p_{n,m}(\mathbf{x}) = \sum_{0 \leq i < j \leq n-1} x_i x_j + x_{n-1} x_n + \sum_{n \leq i < j \leq n+m-1} x_i x_j \tag{14}$$

the number of flat spectra wrt $\{H, N\}$ is as follows:

Lemma 14. *For $n,\ m \geq 1$, we have $K^{HN}_{n,m}$ = # flat spectra$(p_{n,m}(\mathbf{x}))$ wrt $\{H, N\}^n = 3nm - n(\frac{1+(-1)^m}{2}) - m(\frac{1+(-1)^n}{2}) + 3(\frac{1+(-1)^n}{2})(\frac{1+(-1)^m}{2})$*

Proof. The modified adjacency matrix of the graph is as follows:

$$\Gamma_N = \begin{pmatrix} v_0 & 1 & 1 & \dots & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & v_1 & 1 & \dots & 1 & 0 & 0 & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & \dots & v_{n-1} & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & v_n & 1 & 1 & \dots & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & v_{n+1} & 1 & \dots & 1 \\ 0 & 0 & 0 & 0 & 0 & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & \dots & v_{n+m-1} \end{pmatrix}$$

Solving the determinant by minors, we see that $|\Gamma_N| = |G_c| + C$, where G_c is the modified adjacency matrix of the two independent cliques, i.e.,

$$G_c = \begin{pmatrix} v_0 & 1 & 1 & \dots & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & v_1 & 1 & \dots & 1 & 0 & 0 & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & \dots & v_{n-1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & v_n & 1 & 1 & \dots & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & v_{n+1} & 1 & \dots & 1 \\ 0 & 0 & 0 & 0 & 0 & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & \dots & v_{n+m-1} \end{pmatrix}$$

and C is the product of the first $(n-1)\times(n-1)$ minor and the last $(m-1)\times(m-1)$ minor,

$$C = \begin{vmatrix} v_0 & 1 & 1 & \dots & 1 \\ 1 & v_1 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & v_{n-2} \end{vmatrix} \cdot \begin{vmatrix} v_{n+1} & 1 & 1 & \dots & 1 \\ 1 & v_{n+2} & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & v_{n+m-1} \end{vmatrix}$$

The first minor corresponds to the determinant of a clique in $n-1$ variables, say C_1, and the second to that of a clique in $m-1$ variables, say C_2.

As seen in the proof for the number of flat spectra of the clique in n variables wrt $\{H, N\}^n$, here denoted by K_n^c and equal to $n + \frac{1+(-1)^n}{2}$, we have to look separately at the cases when n and m are even or odd:

- Case n, m odd: Here $C = 0$ iff two or more of the $v_0, v_1, \dots, v_{n-2}$ and/or two or more of the $v_{n+1}, v_{n+2}, \dots, v_{n+m-1}$ are equal to 1. In that case $|G_c| = 0$ as well, since there will be linear dependence in the rows in G_c. Therefore the only case in which we obtain $|\Gamma_N| = 1$ is when $C = 1$ and $|G_c| = 0$.
  The number of times $|C_1| = 1$ is K_{n-1}^c, and the number of times $|C_2| = 1$ is K_{m-1}^c. Hence, $C = 1$ in $K_{n-1}^c K_{m-1}^c$ ways and the rank of Γ_N will depend on its rows containing the variables v_{n-1} and v_n. The way to get $|G_c| = 0$ is to make the choice of v_{n-1} and v_n that makes the first and/or second cliques within G_c not flat. Therefore $K_{n,m}^{HN} = K_{n-1}^c(2K_{m-1}^c) + K_{m-1}^c(2K_{n-1}^c - K_{n-1}^c) = 3K_{n-1}^c K_{m-1}^c = 3(n - 1 + \frac{1+(-1)^{n-1}}{2})(m - 1 + \frac{1+(-1)^{m-1}}{2})$
- Case n even, m odd: Here, $C = 0$ as above and also iff $v_0 = v_1 = \dots = v_{n-2} = 0$. In the last case it is possible to have $|G_c| = 1$ iff both cliques within G_c are flat. This happens $2K_m^c$ times: for the first clique we have $v_0 = v_1 = \dots = v_{n-2} = 0$ and so v_{n-1} can be 0 or 1. Adding this to the previous number, we get $3(n - 1 + \frac{1+(-1)^{n-1}}{2})(m - 1 + \frac{1+(-1)^{m-1}}{2}) + 2m + 1 + (-1)^m$.

- Case n odd, m even: As in the previous case, we get $3(n-1+\frac{1+(-1)^{n-1}}{2})(m-1+\frac{1+(-1)^{m-1}}{2})+2n+1+(-1)^n$.
- Case n, m even: In this case we have all the flat spectra of the previous case, plus the independent flat spectra coming from $v_{n+1} = v_{n+2} = \ldots = v_{n+m-1} = 0$ which are not already counted. this number is $2(K^c_{n-1}-2)$. Adding it to the rest we get $3(n-1+\frac{1+(-1)^{n-1}}{2})(m-1+\frac{1+(-1)^{m-1}}{2})+2(m+n-1)+(-1)^m+(-1)^n$.

Summing up and simplifying, we get the desired formula.

Note: The formula is still valid for n or m equal to 1, if we consider $K^c_0 = 1$. □

Fig 5.4.5 summarises our results for the $\{H,N\}^n$ transform set. Further computational results show that, for $n \leq 8$ and $n \leq 5$, the line has the maximum number of flat spectra wrt $\{H,N\}^n$ over the set of quadratics, and over the set of all boolean functions, respectively. We therefore conjecture the following:

Conjecture 1. *The line function, as defined in (12), maximizes the number of flat spectra wrt* $\{H,N\}^n$.

5.3 Bent Properties with respect to the $\{I,H\}^n$-Transform Set

We now investigate certain spectral properties of the boolean functions wrt the $\{I,H\}^n$ transform set, where $\{I,H\}^n$ is the set of 2^n transforms of the form $\bigotimes_{i=0}^{n-1}\{I,H\}$. [35] has investigated other spectral properties wrt $\{I,H\}^n$, such as *weight hierarchy* if the graph is bipartite.

5.3.1 All Graph States are IBent

The WHT of the subspace of a function from $\mathbb{Z}_2^n$to $\mathbb{Z}_2$, obtained by fixing a subset, $\mathbf{R_I}$, of the input variables, can be defined as follows. Let $\theta \in \mathbb{Z}_2^n$ be such that $\theta_j = 1$ iff $j \in \mathbf{R_I}$. Let $\mathbf{r} \preceq \theta$. Then,

$$P_{\mathbf{k},\mathbf{r},\theta} = 2^{-(n-\mathrm{wt}(\theta))/2} \sum_{\mathbf{x}=\mathbf{r}+\mathbf{y}|\mathbf{y}\preceq\bar{\theta}} (-1)^{p(\mathbf{x})+\mathbf{k}\cdot\mathbf{x}} \qquad \mathbf{k} \preceq \bar{\theta}, \mathbf{r} \preceq \theta \tag{15}$$

Given (15) we can define a boolean function as IBent as follows.

Definition 6.

$$p(\mathbf{x}) \textit{ is IBent} \quad \Leftrightarrow \quad \exists\theta \textit{ such that } |P_{\mathbf{k},\mathbf{r},\theta}| = 1 \qquad \forall\mathbf{k} \preceq \bar{\theta}, \forall\mathbf{r} \preceq \theta$$

where $wt(\theta) < \mathbf{n}$.

Let $\mathbf{R_I}$and $\mathbf{R_H}$ be integer sets that partition $\{0,1,\ldots,n-1\}$. Let,

$$U = \bigotimes_{j\in\mathbf{R_I}} I_j \bigotimes_{j\in\mathbf{R_H}} H_j \tag{16}$$

Let,

$$s' = U(-1)^{p(\mathbf{x})} \tag{17}$$

Definition 7. *$p(\mathbf{x})$ is IBent if $\exists$ one or more partitions, $\mathbf{R_I}, \mathbf{R_H}$ such that s' is* flat, *where $|\mathbf{R_I}| < n$.*

An alternative way to define the IBent property of $p(\mathbf{x})$, when $p(\mathbf{x})$ is a quadratic boolean function of n variables, is via the adjacency matrix. Let Γ be the adjacency matrix associated with the quadratic function $p(\mathbf{x})$, and let Γ_I be the adjacency matrix obtained from Γ by deleting all rows and columns of Γ with indices in $\mathbf{R_I}$.

Lemma 15. *For quadratic $p(\mathbf{x})$,*

$$p(\mathbf{x}) \text{ is IBent} \quad \Leftrightarrow \quad \Gamma_I \text{ has maximum rank, mod 2}$$

for one or more choices of $\mathbf{R_I}$ where $|\mathbf{R_I}| < n$.

In general,

$$p(\mathbf{x}) \text{ is Bent} \quad \begin{matrix} \Rightarrow \\ \not\Leftarrow \end{matrix} \quad p(\mathbf{x}) \text{ is IBent}$$

We now state and prove the following Theorem.

Theorem 10. *All boolean functions in two or more variables and of degree ≤ 2 are IBent.*

Proof. Degree zero and degree one functions are trivial. It is easy to show, exhaustively, that all quadratic boolean functions of 2 variables are IBent. The theorem follows by observing that all adjacency matrices, Γ, representing quadratic functions of $n > 2$ variables contain 2×2 submatrices, obtained from Γ by deleting all rows and columns of Γ with indices $\mathbf{R_I}$, for $|\mathbf{R_I}| = n - 2$. □

5.3.2 Not All Boolean Functions are IBent

Lemma 16. *Not all boolean functions of degree > 2 are IBent.*

Proof. By counter-example. For instance, there are no IBent cubics of three variables. □

Further computations show that there are only 416 IBent cubics in four variables (out of a possible $2^{10} - 2^6$), and no IBent quartics in four variables. There are only 442640 IBent cubics, only 1756160 IBent quartics in five variables, and no IBent quintics in five variables. IBent cubics in six variables do exist. Lemma 16 raises an interesting question which we leave as an open problem:

What is the maximum algebraic degree of an IBent boolean function of n variables?

5.3.3 There are No Completely IBent Boolean Functions

A very strict spectral criteria is the Completely IBent criteria. Given (15) we can define a boolean function as Completely IBent as follows. For $\theta \in \mathbb{Z}_2^n$,

Definition 8.

$$p(\mathbf{x}) \text{ is Completely IBent} \Leftrightarrow |P_{\mathbf{k},\mathbf{r},\theta}| = 1 \qquad \forall \theta, \mathbf{k}, \mathbf{r}, \quad \mathbf{k} \preceq \bar{\theta}, \mathbf{r} \preceq \theta$$

Theorem 11. *There are no Completely IBent boolean functions.*

Proof. Let $s = (-1)^{p(\mathbf{x})}$. Let $|\mathbf{R_I}| = n - 1$. Then it is easy to see that any bipolar vector subject to the transform U, as defined in (16), cannot have a flat spectra. □

5.3.4 On the Number of Flat Spectra of Quadratic Boolean Functions with respect to $\{I, H\}^n$

It is of interest to construct boolean functions such that a large subset of the 2^n $\{I, H\}^n$ spectra are flat. Note that [4] defines the interlace polynomial, $q(x)$, for a graph. One can show that $q(1)$ gives the number of flat spectra wrt $\{I, H\}^n$.

The *clique function*, as defined in (13) satisfies the following Lemma.

Lemma 17.

$$\#\ \textit{flat spectra}(p_c(\mathbf{x}))\ \textit{wrt}\ \{I, H\}^n = 2^{n-1}$$

Proof. It is easy to show from its adjacency matrix that the clique function of n variables is Bent for n even. Consider the sub-functions of the n-variable clique function, obtained by fixing a subset of the input variables, $\mathbf{R_I}$. These sub-functions will also be cliques and will be Bent iff $n - |\mathbf{R_I}|$ is even. The Lemma follows by straightforward counting arguments. □

Remark: This clique result appears in [4] as the evaluation of the interlace polynomial $q(x)$ for a *complete graph*at $x = 1$.

The number of flat spectra of the *line* function, as defined by (12), with respect to $\{I, H\}^n$, is precisely the Fibonacci recurrence:

Lemma 18. $K_n^{IH} = \#\ \textit{flat spectra}(p_l(\mathbf{x}))\ \textit{wrt}\ \{I, H\}^n = K_{n-1}^{IH} + K_{n-2}^{IH}$ *with* $K_0^{IH} = K_1^{IH} = 1$*; in closed form,*

$$\frac{(1+\sqrt{5})^{n+1} + (1-\sqrt{5})^{n+1}}{2^{n+1}\sqrt{5}}$$

Proof. Following the same arguments as used later in the proof of Lemma 25, we arrive at the formula:

$$K_n^{IH} = K_n^H + \sum_{i=0}^{n-1} K_{n-1-i}^H K_i^{IH}$$

where K_i^H is the number of flat spectra in i variables wrt. $\{H\}^n$. It is easy to see that $K_n^H = \frac{1+(-1)^n}{2}$. For the rest of the proof, we are going to omit the superscript H and use that $K_n + K_{n+1} = 1$.

Using the recurrence formula for the K_n^{IH} we get

$$\begin{aligned}
K_{n+2}^{IH} &= K_{n+2} + \textstyle\sum_{i=0}^{n+1} K_{n+1-i} K_i^{IH} \\
&= K_{n+2} + \textstyle\sum_{i=0}^{n} K_{n+1-i} K_i^{IH} + K_0 K_{n+1}^{IH} \\
&= K_{n+2} + \textstyle\sum_{i=0}^{n} K_{n+1-i} K_i^{IH} + K_{n+1} + \sum_{i=0}^{n} K_{n-i} K_i^{IH} \\
&= K_{n+1} + K_{n+2} + \textstyle\sum_{i=0}^{n} K_i^{IH} (K_{n-i} + K_{n+1-i}) \\
&= 1 + \textstyle\sum_{i=0}^{n} K_i^{IH}
\end{aligned}$$

and

$$\begin{aligned} K_n^{IH} + K_{n+1}^{IH} &= K_n + K_{n+1} + \sum_{i=0}^{n-1} K_{n-1-i} K_i^{IH} + \sum_{i=0}^{n} K_{n-i} K_i^{IH} \\ &= 1 + \sum_{i=0}^{n-1} K_i^{IH} (K_{n-1-i} + K_{n-i}) + K_n^{IH} K_0 \\ &= 1 + \sum_{i=0}^{n-1} K_i^{IH} + K_n^{IH} \\ &= 1 + \sum_{i=0}^{n} K_i^{IH} \\ &= K_{n+2}^{IH} \end{aligned}$$

This gives us the recurrence relation. Solving it by MAPLE 8, we get the closed formula. □

Remark: This line result appears in [4] as the evaluation of the interlace polynomial $q(x)$ for a *path graph* at $x = 1$.

For the combined graph clique-line-clique, as defined in (14), we get:

Lemma 19. *$K_{n,m}^{IH}$ = # flat spectra($p_{n,m}(\mathbf{x})$) wrt $\{I, H\}^n = 2K_{n-1,m}^{IH} = 2K_{n,m-1}^{IH}$, $n \geq 4$; in closed form,*

$$K_{n,m}^{IH} = 5 \cdot 2^{n+m-4}$$

Proof. Firstly, note that by fixing one of the "connecting" variables, x_{n-1} or x_n, we get two independent cliques, in $n-1$ and m variables respectively or n and $m-1$. On the other hand, if we fix any of the other variables instead, we get the same kind of graph clique-line-clique. We also observe that $p_{n,m}$ is bent iff $n+m$ is even (see next proof).

By the first and second observation, and considering that the order in which we fix doesn't matter, we can write two separate cases:

- Case 1: We can fix any variables but the connecting ones. Then, for the second and third observation, we have flat spectra by fixing t variables iff $n+m-2-t$ is even; that is, if $n+m-t$ is even. Therefore the number of flat spectra for this case is:

$$N1 = \begin{cases} \sum_{k=0}^{(n+m)/2} \binom{n+m-2}{2k}, & n+m \text{ even} \\ \sum_{k=0}^{(n+m-1)/2} \binom{n+m-2}{2k+1}, & n+m \text{ odd} \end{cases}$$

- Case 2: We fix first any of the connecting variables; w.l.o.g., we fix x_{n-1}. We have thus two independent cliques, one of $n-1$ variables and the other of m variables. We have flat spectra by fixing t_1 variables in the first clique and t_2 in the second one iff $n-1-t_1$ and $m-t_2$ are both even. Thus,

$$K_2 = 2^{n-2} 2^{m-1}$$

- Case 3: We fix first x_n and any of the remaining variables but x_{n-1}. We get then two independent cliques, one of n variables and the other of $m-1$

variables. We have flat spectra by fixing t_1 variables in the first clique and t_2 in the second one iff $n-1-t_1$ and $m-t_2$ are both even. Thus,

$$N3 = 2^{m-2} \cdot \begin{cases} \sum_{k=0}^{(n-1)/2} \binom{n-1}{2k}, & n \text{ odd} \\ \sum_{k=0}^{(n-2)/2} \binom{n-1}{2k+1}, & n \text{ even} \end{cases}$$

We have that $K^{IH}_{n,m} = N1 + N2 + N3$; in principle, the result depends on the parity of n and m. However

$$\sum_{k=0}^{s/2} \binom{s}{2k} = 1 + \sum_{k=1}^{s/2} \left[\binom{s-1}{2k} + \binom{s-1}{2k-1} \right] = 1 + \sum_{i=1}^{s-1} \binom{s-1}{i} = 2^{s-1}$$

and in the same way

$$\sum_{k=0}^{(s-1)/2} \binom{s}{2k+1} = \sum_{k=1}^{(s-1)/2} \left[\binom{s-1}{2k+1} + \binom{s-1}{2k} \right] = \sum_{i=0}^{s-1} \binom{s-1}{i} = 2^{s-1}$$

Therefore, in all cases, we get $K^{IH}_{n,m} = N1 + N2 + N3 = 5 \cdot 2^{n+m-4}$, and from here, trivially, the recurrence relation. □

Fig 5.4.5 summarises our results for the $\{I, H\}^n$ transform set. Computational results show that, for $n \leq 8$ and $n \leq 5$, the clique function has the maximum number of flat spectra wrt $\{I, H\}^n$ over the set of quadratics and over the set of all boolean functions, respectively. We therefore conjecture the following.

Conjecture 2. *The clique function, as defined in (13), maximises the number of flat spectra wrt* $\{I, H\}^n$.

5.4 Bent Properties with respect to the $\{I, H, N\}^n$-Transform Set

5.4.1 All Graph States are IBent$_4$

The $\{H, N\}^{n-|\mathbf{R_I}|}$ set of transforms of the subspace of a function from $\mathbb{Z}_2^n$to $\mathbb{Z}_2$, obtained by fixing a subset, $\mathbf{R_I}$, of the input variables, can be defined as follows. Let $\theta \in \mathbb{Z}_2^n$ be such that $\theta_j = 1$ iff $j \in \mathbf{R_I}$. Let $\mathbf{r} \preceq \theta$. Then,

$$P_{\mathbf{k},\mathbf{c},\mathbf{r},\theta} = 2^{-(n-\mathrm{wt}(\theta))/2} \sum_{\mathbf{x}=\mathbf{r}+\mathbf{y}|\mathbf{y}\preceq\bar{\theta}} (i)^{2[p(\mathbf{x})+\mathbf{k}\cdot\mathbf{x}]+[\mathbf{c}\cdot\mathbf{x}]} \qquad \mathbf{k}, \mathbf{c} \preceq \bar{\theta}, \mathbf{r} \preceq \theta \tag{18}$$

Given (18) we can define a boolean function as IBent$_4$ as follows.

Definition 9.

$$p(\mathbf{x}) \textit{ is IBent}_4 \quad \Leftrightarrow \quad \exists \mathbf{c}, \theta \textit{ such that } |P_{\mathbf{k},\mathbf{c},\mathbf{r},\theta}| = 1 \qquad \forall \mathbf{k} \preceq \bar{\theta}, \forall \mathbf{r} \preceq \theta$$

where $wt(\theta) < n$.

Let $\mathbf{R_I}$, $\mathbf{R_H}$ and $\mathbf{R_N}$ be integer sets that partition $\{0, 1, \ldots, n-1\}$. Let,

$$U = \bigotimes_{j\in\mathbf{R_I}} I_j \bigotimes_{j\in\mathbf{R_H}} H_j \bigotimes_{j\in\mathbf{R_N}} N_j \tag{19}$$

Let,

$$s' = U(-1)^{p(\mathbf{x})} \tag{20}$$

Lemma 20. *$p(\mathbf{x})$ is IBent$_4$ if $\exists$ one or more partitions, $\mathbf{R_I}, \mathbf{R_H}, \mathbf{R_N}$ such that s' is* flat, *where $|\mathbf{R_I}| < n$.*

An alternative way to define the IBent$_4$ property of $p(\mathbf{x})$, when $p(\mathbf{x})$ is a quadratic boolean function of n variables, is via the adjacency matrix. Let Γ be the adjacency matrix associated with the quadratic function $p(\mathbf{x})$, and let Γ_I be the adjacency matrix obtained from Γ by deleting all rows and columns of Γ with indices in $\mathbf{R_I}$.

Lemma 21. *For quadratic $p(\mathbf{x})$,*

$$p(\mathbf{x}) \text{ is IBent}_4 \quad \Leftrightarrow \quad \Gamma_I + diag(v) \text{ has maximum rank, mod 2,} \quad \text{where } v \preceq \bar{\theta}$$

for one or more choices of v and θ where $wt(\theta) < n$.

In general,

$$p(\mathbf{x}) \text{ is Bent} \begin{array}{c} \Rightarrow \\ \not\Leftarrow \\ \Rightarrow \\ \not\Leftarrow \end{array} \begin{array}{l} p(\mathbf{x}) \text{ is Bent}_4 \quad \Rightarrow \\ p(\mathbf{x}) \text{ is IBent} \quad \not\Leftarrow \end{array} p(\mathbf{x}) \text{ is IBent}_4$$

The following is a straightforward corollary.

Theorem 12. *All boolean functions of degree ≤ 2 are IBent$_4$.*

Proof. This follows from Theorems 7 and 10. □

5.4.2 All Boolean Functions are IBent$_4$

Lemma 22. *All boolean functions are IBent$_4$.*

Proof. In Section 4.3 it is apparent, from Theorem 5 that the action of U_v on a boolean function, $p(\mathbf{x})$, of any degree, always gives a flat output spectra, for any value of v. This gives (at least) n flat spectra for any boolean function. □

5.4.3 There are No Completely IBent$_4$ Boolean Functions

An extremely strict spectral criteria is the Completely IBent criteria. Given (15) we define a boolean function as Completely IBent$_4$ as follows. For $\theta \in \mathbb{Z}_2^n$,

Definition 10.

$$p(\mathbf{x}) \text{ is Completely IBent}_4 \Leftrightarrow |P_{\mathbf{k},\mathbf{c},\mathbf{r},\theta}| = 1 \qquad \forall \theta, \mathbf{c}, \mathbf{k}, \mathbf{r}, \quad \mathbf{k}, \mathbf{c} \preceq \bar{\theta}, \mathbf{r} \preceq \theta$$

Theorem 13. *There are no Completely IBent$_4$ boolean functions.*

Proof. Neither Theorems 9 or 11 are satisfied. □

5.4.4 Not All Graph States are 'LC-Bent'

In the context of LC, a natural question to ask is whether, for a given quadratic boolean function, $p(\mathbf{x})$, there exists at least one quadratic boolean function within its LC orbit which is Bent. If so, then we state that the graph state, $p(\mathbf{x})$, and its associated LC-orbit, is *LC-Bent*. More formally,

Definition 11. *The graph state, $p(\mathbf{x})$ (a boolean quadratic function), and its associated LC-orbit is* LC-Bent *if $\exists p'(\mathbf{x})$ such that $p'(\mathbf{x}) \in LC\ Orbit(p(\mathbf{x}))$, and such that $p'(\mathbf{x})$ is a Bent boolean function.*

For example, the Bent boolean function $x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3$ is in the same LC orbit as $x_0x_1 + x_0x_2 + x_0x_3$ so, although $x_0x_1 + x_0x_2 + x_0x_3$ is not Bent, it is LC-Bent.

In general, for $p(\mathbf{x})$ quadratic,

$$p(\mathbf{x}) \text{ is Bent } \begin{array}{c} \Rightarrow \\ \not\Leftarrow \end{array} \quad p(\mathbf{x}) \text{ is LC-Bent}$$

It is not at all obvious that there exist LC-orbits which do not contain at least one Bent representative. However it turns out that such orbits do exist.

Theorem 14. *Not all quadratic boolean functions are LC-Bent.*

Proof. By computation, the LC-orbit associated with the $n = 6$-variable boolean function, $x_0x_4 + x_1x_5 + x_2x_5 + x_3x_4 + x_4x_5$ is not LC-Bent. □

By computation it was found that all quadratic boolean functions of $n \leq 5$ variables are LC-Bent. Table 5.4.4 lists orbit representatives for those orbits which are not LC-Bent, for $n = 2$ to 9, and provides a summary for $n = 10$, where the boolean functions are abbreviated so that, say, ab, de, fg is short for $x_ax_b + x_dx_e + x_fx_g$. For those orbits which are not LC-Bent we provide the maximum rank satisfied by a graph within the orbit.

n	ANF for the orbit representative	Max. Rank within Orbit
2-5	-	-
6	04,15,25,34,45	4
7	-	-
8	07,17,27,37,46,56,67	6
	06,17,27,37,46,56,67	6
	07,17,25,36,46,57,67	6
	06,17,27,36,45,46,47,56,57,67	6
	07,16,26,35,45,47,67	6
9	08,18,28,38,47,57,67,78	6
	08,18,26,37,47,56,68,78	6
10	08,19,29,39,49,58,68,78,89	6
	51 other orbits	8

Table 1: Representatives for all LC-Orbits which are not LC-Bent for $n = 2$ to 10

5.4.5 On the Number of Flat Spectra of Boolean Functions with respect to $\{I, H, N\}^n$

It is of interest to construct boolean functions such that a largest subset of the 3^n $\{I, H, N\}^n$ spectra are flat. As a means of comparison, we first consider the number of flat spectra for the near-worst and worst-case functions, namely the constant function and the single monomial function of degree n, respectively.

Lemma 23. *The constant function $p(\mathbf{x}) = 0$ or 1 has 2^n flat spectra with respect to $\{I, H, N\}^n$ (including the identity transformation).*

Proof. Any $\{I, N\}^n$ transform of the constant function is flat, and none of the others: As an obvious generalization of (5.2.1), we get flat spectra iff

$$A_{k,R_H,R_N,R_I} = \sum_{\mathbf{x}\in S}(-1)^{p_I(\mathbf{x})+p_I(\mathbf{x}+\mathbf{k})+\sum_{i=1}^{n-1}\chi_{\mathbf{R_N}}(i)k_ix_i+\sum_{i=1}^{n-1}\chi_{\mathbf{R_N}}(i)k_i} = 0, \qquad \forall \mathbf{k} \neq \mathbf{0}$$

where $S = \{0, \ldots, n-1\} \setminus \mathbf{R_I}$, and p_I is the function p with the variables x_i such that $i \in \mathbf{R_I}$ are fixed. That is true iff $p_I(\mathbf{x}) + p_I(\mathbf{x}+\mathbf{k}) + \sum_{i=1}^{n-1}\chi_{\mathbf{R_N}}(i)k_ix_i + \sum_{i=1}^{n-1}\chi_{\mathbf{R_N}}(i)k_i$ is a balanced function for all $\mathbf{k} \neq \mathbf{0}$, or, equivalently, if $p_I(\mathbf{x}) + p_I(\mathbf{x}+\mathbf{k}) + \sum_{i=1}^{n-1}\chi_{\mathbf{R_N}}(i)k_ix_i$ is balanced. In our case, for any choice of $\mathbf{R_I}$, we get $p_I(\mathbf{x}) = p(\mathbf{x}) = 0$. Thus, we get flat spectra iff $\sum_{i=1}^{n-1}\chi_{\mathbf{R_N}}(i)k_ix_i$ is balanced for all $\mathbf{k} \neq \mathbf{0}$. Clearly, if all $\chi_{\mathbf{R_N}}(i) = 1$, we get a balanced function for all $\mathbf{k} \neq \mathbf{0}$. But if any of the $\chi_{\mathbf{R_N}}(i) = 0$, by taking $k = (0, \ldots, 1, \ldots, 0)$, where the 1 is in the position i, we get an unbalanced function. □

Lemma 24. *The single degree-n monomial function, $p(\mathbf{x}) = x_0x_1x_2\ldots x_{n-1}$, has $n+1$ flat spectra wrt $\{I, H, N\}^n$ (including the identity transformation), except for the case $n = 2$. This is the minimal number of flat spectra possible for a boolean function wrt $\{I, H, N\}^n$.*

Proof. If $n = 1$, then the monomial function becomes the linear function x_0 in one variable. This will have the same flat spectra as the constant function in one variable, i.e. $2^1 = 2 = n + 1$. The single monomial for $n = 2$ is the line in two variables, so its flat spectra have been established before in this paper. When $p(\mathbf{x}) = x_0x_1\cdots x_{n-1}$,

$$p(\mathbf{x}) + p(\mathbf{x}+\mathbf{k}) + \sum_{i=1}^{n-1}\chi_{\mathbf{R_N}}(i)k_ix_i = \sum_{i=0}^{n-1}k_ix_0\cdots x_{i-1}x_{i+1}\cdots x_n +$$
$$+ \sum_{j>i}k_ik_jx_0x_0\cdots x_{i-1}x_{i+1}\cdots x_{j-1}x_{j+1}\cdots x_n + \ldots + k_0k_1\cdots k_{n-1} + \sum_{i=1}^{n-1}\chi_{\mathbf{R_N}}(i)k_ix_i$$

For $n > 2$ we take $k = (1, 0, \ldots, 0)$. The above function is then $x_1\cdots x_{n-1} + \chi_{\mathbf{R_N}}(0)x_0$, which is balanced iff $\chi_{\mathbf{R_N}}(0) = 1$. Similarly, we see that we must have $\chi_{\mathbf{R_N}}(i) = 1, 0 \leq i \leq n-1$. Take $k = (1, 1, 0\ldots, 0)$. The function we get now is $x_1\cdots x_{n-1} + x_0x_2\cdots x_{n-1} + x_2\cdots x_{n-1} + x_0 + x_1$, which is not balanced. Therefore, for $n > 2$, we need to fix at least $n-2$ variables in order to obtain flat spectra; that is, we need $|\mathbf{R_I}| \geq n-2$. Suppose now $|\mathbf{R_I}| = n-2$: By symmetry, we can suppose, w.l.o.g., that we fix $x_2, \ldots, x_{n-1}$. If we fix any of the $x_i = 0$, then our new function is a constant, $p_I = 0$. As we have just seen, the only possibility for $p_I(\mathbf{x}) + p_I(\mathbf{x}+\mathbf{k}) + \chi_{\mathbf{R_N}}(0)k_0x_0 + \chi_{\mathbf{R_N}}(1)k_1x_1$ to be balanced for all $k \neq (0, 0)$ is that $\chi_{\mathbf{R_N}}(0) = \chi_{\mathbf{R_N}}(1) = 1$. On the other hand, if we fix $x_i = 1\ \forall i \geq 2$, $p_I = x_0x_1$, the line in two variables; as we can easily deduce from the modified adjacency matrix, is flat iff $\chi_{\mathbf{R_N}}(i) = 0$ for at least one of the i's. Thus we get a contradiction, so in

fact $|\mathbf{R_I}| \geq n-1$. When $|\mathbf{R_I}| = n-1$, by fixing we get now either $p_I = 0$ or $p_I = x_i$. Both have a flat spectrum iff $\chi_{\mathbf{R_N}}(i) = 1$, so from here we get n flat spectra. For $|\mathbf{R_I}| = n$, we get another flat spectrum, and that completes the proof. □

Although the line function of (12) appears to give the maximal number of flat spectra wrt $\{H,N\}^n$, it does not do so well wrt $\{I,H,N\}^n$. We now show that the number of flat spectra wrt $\{I,H,N\}^n$ for the construction of (12) satisfies,

Lemma 25. *K_n^{IHN} = # flat spectra$(p_l(\mathbf{x}))$ wrt $\{I,H,N\}^n = 2(K_{n-1}^{IHN} + K_{n-2}^{IHN})$ with $K_0^{IHN} = 1$ and $K_1^{IHN} = 2$; in closed form,*

$$K_n^{IHN} = \frac{(1+\sqrt{3})^{n+1} - (1-\sqrt{3})^{n+1}}{2\sqrt{3}}$$

Proof. We are first going to see that

$$K(k) = \sum_{\sum_{\lambda=0}^{k} v_\lambda = n-k} \prod_{j=0}^{k} K_{v_j}$$

where $K(k)$ is the number of flat spectra when $|R_I| = k$, and K_a is the number of flat spectra in a variables wrt $\{H,N\}^n$.

Let $R_I = \{i_0, \ldots, i_{k-1}\}$. Then,

$$D(k) = \det(\Gamma_I + \ \mathrm{diag}(v)) = D^{0,\ldots,i_0-1} D^{i_0+1,\ldots,i_1-1} \cdots D^{i_k+1,\ldots,n-1}$$

where $D^{k_0,\ldots,k_t}$ is the determinant of the modified matrix of the line, $\Gamma + \ \mathrm{diag}(v)$, in the variables $x_{k_0}, \ldots, x_{k_t}$ (when the indices are consecutive, we consider the corresponding determinant to be 1). To prove this formula we use induction on k.

Case $k = 0$ ($R_I = \emptyset$). Evidently, $D(0) = D^{0,\ldots,n-1}$.

Case $k = 1$. In this case $R_I = \{i_0\}$. When we 'cross out' from the matrix the i_0th row and column, we get a block matrix of four blocks in which both antidiagonal blocks are zero. $D(1) = 1$ if and only if the rows of the matrix are linearly independent. But because of the antidiagonal blocks being zero, that happens if and only if in each of the other two blocks the rows are linearly independent. That is, $D(1) = D^{0,\ldots,i_0-1} D^{i_0+1,\ldots,n-1}$

Suppose it is true for $|R_I| = m$; that is, for $R_I = \{j_0, \ldots, j_{m-1}\}$, $D(m) = D^{0,\ldots,j_0-1} \cdots D^{j_m+1,\ldots,n-1}$. We will see that it is true for $|R_I| = m+1$:

Let $R_I = \{i_0, \ldots, i_m\} = \{j_0, \ldots, j_l, \lambda, j_{l+1}, \ldots, j_{m-1}\}$. Then, by induction hypothesis $D(m+1) = D^{0,\ldots,j_0-1} \cdots D_\lambda^{j_l+1,\ldots,j_{l+1}-1} \cdots D^{j_{m-1}+1,\ldots,n-1}$, where $D_\lambda^{j_l+1,\ldots,j_{l+1}-1}$ represents the determinant $D^{j_l+1,\ldots,j_{l+1}-1}$ with the λth row and column crossed out. By the case $k = 1$, we see that

$$D_\lambda^{j_l+1,\ldots,j_{l+1}-1} = D^{j_l+1,\ldots,\lambda-1} D^{\lambda+1,\ldots,j_{l+1}-1}$$

and that concludes the proof of the formula for the determinants.

The determinant is 1 if and only if each one of the determinants is 1. But each determinant $D^{k_0,\ldots,k_t}$ will be 1 exactly $K_{k_t-k_0+1}$ times. So for $R_I = \{i_0, \ldots, i_k\}$, the number of flat spectra is $K = K_{i_0} K_{i_1-i_0-1} \cdots K_{n-1-i_k}$ (when the indices are consecutive, we get $K_0 = 1$) and so

$$K(k) = \sum_{|R_I|=k} K_{i_0} K_{i_1-i_0-1} \cdots K_{n-1-i_k}.$$

The summands that appear in $K(k)$ are all possible products $\prod K_i$ such that the sum of the indices is $n-k$, so we have

$$K(k) = \sum_{\sum_{\lambda=0}^{k} v_\lambda = n-k} \prod_{j=0}^{k} K_{v_j}$$

If we write the indices as a vector, $(v_0, \ldots, v_{n-1})$, where $\sum_{l=0}^{n-1} v_l = n-k$, then for $(v_1, \ldots, v_{n-1})$ we have that $\sum_{l=1}^{n-1} v_l = n-k-v_0$. Hence, for all possible vectors in $K_n^{IHN} = \sum_{k=0}^{n-1} K(k)$ we have all possible vectors in the lesser indices, as follows:

$$K_n^{IHN} = K_n + K_{n-1}K_0^{IHN} + K_{n-2}K_1^{IHN} + \ldots + K_0 K_{n-1}^{IHN} = K_n + \sum_{i=0}^{n-1} K_{n-1-i}K_i^{IHN}$$

In the sequel we are going to use that $K_n = 2^n - K_{n-1}$ (see Lemma 5.2.4), or more accurately its consequence $K_{n+1} + K_{n+2} = 2^{n+2} = 2(K_n + K_{n+1})$; also, we will use that $K_0 = K_1 = 1$.

Using the recurrence formula for the K_n^{IHN} we get

$$2K_n^{IHN} + 2K_{n+1}^{IHN} = 2K_n + 2K_{n+1} + 2\sum_{i=0}^{n-1} K_{n-1-i}K_i^{IHN} + 2\sum_{i=0}^{n} K_{n-i}K_i^{IHN}$$

This is equal to

$$\begin{aligned}
&K_{n+2} + K_{n+1} + \textstyle\sum_{i=0}^{n-1} K_i^{IHN} 2(K_{n-1-i} + K_{n-i}) + 2K_n^{IHN}K_0 = \\
&K_{n+2} + \textstyle\sum_{i=0}^{n-1} K_i^{IHN}(K_{n-i} + K_{n-i+1}) + K_n^{IHN}(K_0 + K_1) + K_{n+1} = \\
&K_{n+2} + \textstyle\sum_{i=0}^{n} K_i^{IHN}(K_{n-i} + K_{n-i+1}) + K_{n+1} = \\
&K_{n+2} + \textstyle\sum_{i=0}^{n} K_i^{IHN}K_{n-i+1} + K_{n+1} + \sum_{i=0}^{n} K_i^{IHN}K_{n-i} = \\
&K_{n+2} + \textstyle\sum_{i=0}^{n} K_i^{IHN}K_{n-i+1} + K_{n+1}^{IHN} = \\
&K_{n+2} + \textstyle\sum_{i=0}^{n+1} K_i^{IHN}K_{n-i+1} = K_{n+2}^{IHN}
\end{aligned}$$

Solving by MAPLE 8, we get the closed formula. □

Remark: This result can be gleaned, indirectly, from page 23 of [1] as the evaluation of the interlace polynomial $Q(x)$ for the path graph at $x = 2$.

Although the clique function as defined in (13) appears to be maximal wrt $\{I, H\}^n$, it does not do so well wrt $\{I, H, N\}^n$. We now show that the number of flat spectra wrt $\{I, H, N\}^n$ for the construction of (13) satisfies,

Lemma 26. *K_n^{IHN} = # flat spectra($p_c(\mathbf{x})$) wrt $\{I, H, N\}^n = 2K_{n-1}^{IHN} + 2^n$; in closed form,*

$$K_n^{IHN} = 2^n + (n-1)2^{n-1}$$

Proof. As stated, if we have a clique in n variables and we fix a subset in the input of variables (that is, we choose $\mathbf{R_I}$), we get a clique in $n - |\mathbf{R_I}|$ variables. Thereby, for each selection of $\mathbf{R_I}$ we have as many flat spectra as the number of flat spectra wrt $\{H, N\}^{n-|\mathbf{R_I}|}$, in $n - |\mathbf{R_I}|$ variables. So:

$$\#\text{ flat spectra}(p_c(\mathbf{x}))\text{ wrt }\{I, H, N\}^n = \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) K_{n-i}$$

where K_{n-i} is the number of flat spectra of the clique in $n-i$ variables wrt $\{H,N\}^{n-i}$.

$$\sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right) K_{n-i} = \sum_{i=0}^{n}\left(\begin{array}{c} n \\ n-i \end{array}\right) K_i = \sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right) K_i =$$
$$\sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right)\left(i+\frac{1+(-1)^i}{2}\right) =$$
$$\sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right) i + \sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right)\frac{1}{2} + \sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right)\frac{(-1)^i}{2} =$$
$$\sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right) i + 2^{n-1} + 0$$

Taking the first term,

$$\sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right) i = \left(\begin{array}{c} n \\ 0 \end{array}\right) 0 + \left(\begin{array}{c} n \\ n \end{array}\right) n + \sum_{i=1}^{n-1}\left(\begin{array}{c} n \\ i \end{array}\right) i =$$
$$n + \sum_{i=1}^{n-1}\left[\left(\begin{array}{c} n-1 \\ i \end{array}\right) + \left(\begin{array}{c} n-1 \\ i-1 \end{array}\right)\right] i = n + \sum_{i=0}^{n-1}\left(\begin{array}{c} n-1 \\ i \end{array}\right) i + \sum_{i=0}^{n-1}\left(\begin{array}{c} n-1 \\ i-1 \end{array}\right) i =$$
$$n + 2\sum_{i=0}^{n-1}\left(\begin{array}{c} n-1 \\ i \end{array}\right) i - \left(\begin{array}{c} n-1 \\ n-1 \end{array}\right)(n-1) + \sum_{i=0}^{n-2}\left(\begin{array}{c} n-1 \\ i \end{array}\right) =$$
$$2\sum_{i=0}^{n-1}\left(\begin{array}{c} n-1 \\ i \end{array}\right) + 1 + 2^{n-1} - \left(\begin{array}{c} n-1 \\ n-1 \end{array}\right)$$

Substituting, we get that $K_n^{IHN} = 2K_{n-1}^{IHN} + 2^n$. From the recurrence relation we get the desired formula. □

Remark: K_n^{IHN} for the clique function (*complete graph*) for $n = 2$ to 4 can be found on page 21 of [1] by evaluating the interlace polynomial $Q(x)$ for the complete graph at $x = 2$.

As for the clique-line-clique structure, as defined in (14), the number of flat spectra is as follows:

Lemma 27. $K_{n,m}^{IHN} = \#$ *flat spectra*$(p_{n,m}(\mathbf{x}))$ *wrt* $\{I,H,N\}^n = 2^{n+m-3}(3nm + 2n + 2m + 2)$

Proof. Suppose that one or both of the connecting variables are in $\mathbf{R_I}$: when we fix one of the connecting variables, we get two independent cliques, so from this case we get

$$K_{n-1,C}^{IHN}K_{m,C}^{IHN} + K_{n,C}^{IHN}K_{m-1,C}^{IHN} - K_{n-1,C}^{IHN}K_{m-1,C}^{IHN} = 2^{m+n-4}(3nm + 2n + 2m)$$

where $K_{k,C}^{IHN}$ is the number of flat spectra of the clique in k variables.

On the other hand, when none of the connecting variables are in $\mathbf{R_I}$, we get another clique-line-clique: suppose that we fix i variables in the first clique and j in the second one. In that case, we will have as many flat spectra as the number of flat spectra wrt $\{H,N\}$ of a $(n-i)$ clique - 1 line - $(m-j)$ clique. Considering all possible fixings in this case, we get:

$$\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}\left(\begin{array}{c} n-1 \\ i \end{array}\right)\left(\begin{array}{c} m-1 \\ j \end{array}\right) K_{n-i,m-j}^{HN} =$$
$$\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}\left(\begin{array}{c} n-1 \\ i \end{array}\right)\left(\begin{array}{c} m-1 \\ j \end{array}\right)\left[3(n-i)(m-j) - (n-i)(\tfrac{1+(-1)^{m-j}}{2}) -\right.$$
$$\left. -(m-j)(\tfrac{1+(-1)^{n-i}}{2}) + 3(\tfrac{1+(-1)^{n-i}}{2})(\tfrac{1+(-1)^{m-j}}{2})\right] = 2^{m+n-4}(3nm + 2n + 2m + 4)$$

□

It turns out that high-distance stabilizer quantum codes (optimal additive codes over GF(4)) are ideal candidates for quadratic boolean functions with large numbers of flat spectra wrt $\{I, H, N\}^n$. Exhaustive computer search for $n = 4$ to $n = 9$-variable quadratic boolean functions finds one unique LC orbit of functions for each n whose number of flat spectra with respect to $\{I, H, N\}^n$ is optimal, and a representative for each of these orbits is listed in Table 5.4.5. These functions all map to additive zero-dimension QECCs with optimal distances, as shown in Table 5.4.5 (see [26]). It remains open as to whether the quadratic function with the optimal number of flat spectra wrt $\{I, H, N\}^n$ will always have optimal distance when viewed as a QECC, and vice versa. In any case, the approximate correspondence is to be expected as the QECC distance is equal to the *aperiodic propagation criteria (APC) distance* of the quadratic boolean functions, as presented in [17], and optimal propagation (aperiodic autocorrelation) criteria will relate to very good spectral properties via a generalised form of Fourier duality. Tables 5.4.5 to 5.4.5 show an exhaustive computer search for boolean functions that achieve the optimal number of flat spectra wrt $\{I, H, N\}^n$ for cubics, quartics, and quintics, respectively, where one representative function is given per LC orbit. As expected the maximum number of flat spectra decreases as algebraic degree of the boolean function rises. Also shown is the distance of the boolean function when viewed as a zero-dimensional QECC. As with the quadratics, this distance parameter can be interpreted as the APC distance of a boolean function (see [17] for more details). In all cases the boolean functions shown in the tables achieve the maximum possible distance for their given algebraic degree.

Function	Monomial ($n > 2$)	Constant	Line	Clique	Clique-Line-Clique
ANF	$x_0 \ldots x_{n-1}$	1	$\sum_{j=0}^{n-2} x_j x_{j+1}$	$\sum_{0 \le i < j \le n-1} x_i x_j$	$\sum_{0 \le i < j \le n-1} x_i x_j + x_{n-1} x_n + \sum_{n \le i < j \le n+m-1} x_i x_j$
K_n^{HN}	0	2^n	$\frac{1}{3}\left(2^{n+1} + (-1)^n\right)$	$n + \frac{1+(-1)^n}{2}$	$3nm - n(\frac{1+(-1)^m}{2}) - m(\frac{1+(-1)^n}{2}) + 3(\frac{1+(-1)^n}{2})(\frac{1+(-1)^m}{2})$
K_n^{IH}	1	1	$\frac{(1+\sqrt{5})^{n+1}+(1-\sqrt{5})^{n+1}}{2^{n+1}\sqrt{5}}$	2^{n-1}	$5 \cdot 2^{n+m-4}$
K_n^{IHN}	$n+1$	2^n	$\frac{(1+\sqrt{3})^{n+1}-(1-\sqrt{3})^{n+1}}{2\sqrt{3}}$	$2^n + (n-1)2^{n-1}$	$2^{n+m-3}(3nm + 2n + 2m + 2)$

Table 2: The Maximum Number of Flat Spectra wrt $\{I, H, N\}^n$ for Quadratic Boolean Functions

n	distance	Quadratics Optimal for K_n^{IHN}	K_n^{IHN}	K_n^{IHN} for the line
4	2	02,13,23	44	44
5	3	01,02,13,24,34	132	120
6	4	01,02,05,13,15,24,25,34,35,45	396	328
7	3	03,06,14,16,25,26,34,35,45	1096	896
8	4	02,03,04,12,13,15,26,37,46,47,56,57,67	3256	2448
9	4	04,07,08,14,16,18,25,26,28,34,35,37,57,58,67,68	9432	6688

Table 3: The Maximum Number of Flat Spectra wrt $\{I, H, N\}^n$ for Quadratic Boolean Functions

n	distance	Cubics Optimal for K_n^{IHN}	K_n^{IHN}
3	1	012	4
4	2	012,03,13,23	20
5	2	012,03,14,23,24	72
6	3	012,03,04,13,15,24,25	248

Table 4: The Maximum Number of Flat Spectra wrt $\{I, H, N\}^n$ for Cubic Boolean Functions

n	distance	Quartics Optimal for K_n^{IHN}	K_n^{IHN}
4	1	All Quartics	5
5	2	0123,01,04,14,23,24,34	30
		0123,02,04,13,14,23,24,34	
		0123,04,14,23,24,34	

Table 5: The Maximum Number of Flat Spectra wrt $\{I, H, N\}^n$ for Quartic Boolean Functions

6 Conclusion

This paper has examined the spectral properties of boolean functions with respect to the transform set formed by tensor products of the identity, I, the Walsh-Hadamard kernel, H, and the Negahadamard kernel, N (the $\{I, H, N\}^n$ transform set). In particular, the idea of a Bent boolean function was generalised in a number of ways to the $\{I, H, N\}^n$ transform set. Various theorems about the generalised Bent properties of boolean functions were established. It was shown how a quadratic boolean function maps to a quantum graph state and it was shown how the local unitary equivalence of these graph states can be realised by the successive application of the LC operation - Local Complementation - or, alternatively, by identifying a subset of the flat spectra with respect to the $\{I, H, N\}^n$ transform set. For quadratic boolean functions it was further shown how the $\{I, H, N\}^n$ set of transform spectra could be characterised by looking at the ranks of suitably modified versions of the adjacency matrix. Simple recursions for the number of flat spectra with respect to $\{I, H, N\}^n$ were also derived for certain recursive quadratic boolean constructions, and it was demonstrated that Quantum Error Correcting Codes with optimal distance appear to have the most flat spectra with respect to $\{I, H, N\}^n$, at least for small n. It was also shown computationally, for small n, that the number of flat spectra decreases with increasing algebraic degree of the boolean function. Future work should seek to establish constructions for boolean functions of degree greater than two that have as large a number of flat spectra as possible with respect to $\{I, H, N\}^n$. More generally, it would be of interest to relax the criteria somewhat, and look for those functions which have many spectra with respect to $\{I, H, N\}^n$ with a worst-case spectral power peak less than some low upper bound (see [18]). One would expect, in this case, that many more boolean functions of degree > 2 would be found that do well for this relaxed criteria.

n	distance	Quintics Optimal for K_n^{IHN}	K_n^{IHN}
5	1	All Quintics	6

Table 6: The Maximum Number of Flat Spectra wrt $\{I, H, N\}^n$ for Quintic Boolean Functions

References

[1] M. Aigner and H. van der Holst, "Interlace Polynomials", *Linear Algebra and its Applications*, **377**, pp. 11–30, 2004.

[2] R. Arratia, B. Bollobas, and G.B. Sorkin, "The Interlace Polynomial: a new graph polynomial", *Proc. 11th Annual ACM-SIAM Symp. on Discrete Math.*, pp. 237–245, 2000.

[3] R. Arratia, B. Bollobas, D. Coppersmith, and G.B. Sorkin, "Euler Circuits and DNA Sequencing by Hybridization", *Disc. App. Math.*, **104**, pp. 63–96, 2000.

[4] R. Arratia, B. Bollobas, and G.B. Sorkin, "The Interlace Polynomial of a Graph", Preprint: http://arxiv.org/abs/math/0209045, v2, 13 Aug. 2004.

[5] R. Arratia, B. Bollobas, and G.B. Sorkin, "Two-Variable Interlace Polynomial", Preprint: http://arxiv.org/abs/math/0209054, v3, 13 Aug. 2004.

[6] H.J. Briegel and R. Raussendorf, "Persistent Entanglement in Arrays of Interacting Particles," *quant-ph/0004051 v2*, 28 Aug 2000.

[7] A. Bouchet, "Isotropic Systems," *European J. Combin.*, **8**, pp. 231–244, 1987.

[8] A. Bouchet, "Transforming trees by succesive local complementations" *J. Graph Theory*, **12**, pp. 195-207, 1988.

[9] A. Bouchet, "Graphic Presentation of Isotropic Systems", *J. Combin. Thoery B*, **45**, pp. 58–76, 1988.

[10] A. Bouchet, "Tutte-Martin Polynomials and Orienting Vectors of Isotropic Systems", *Graphs Combin.*, **7**, pp. 235–252, 1991.

[11] A.R. Calderbank,E.M. Rains,P.W. Shor and N.J.A. Sloane, "Quantum Error Correction Via Codes Over GF(4)," *IEEE Trans. on Inform. Theory,* **44**, pp. 1369–1387, 1998, (preprint: http://xxx.soton.ac.uk/abs/quant-ph/?9608006).

[12] P.J.Cameron, "Cycle Index, Weight Enumerator, and Tutte Polynomial", *Electronic Journal of Combinatorics*, **9**, 2, 2002.

[13] C. Carlet, "Two New Classes of Bent Functions", *Advances in Cryptology - EUROCRYPT'93, Lecture Notes in Computer Science, Springer-Verlag*, Vol 765, pp. 77–101, 1994.

[14] B. Courcelle and S. Oum, "Vertex-minors, MS Logic and Seese's Conjecture", *preprint*, 2004.

[15] L.E. Danielsen, "Database of Self-Dual Quantum Codes", *http://www.ii.uib.no/~larsed/vncorbits/*, 2004.

[16] L.E. Danielsen, *Master's Thesis - in preparation*, Selmer Centre, Inst. for Informatics, University of Bergen, Bergen, Norway, 2004.

[17] L.E. Danielsen,T.A. Gulliver and M.G. Parker, "Aperiodic Propagation Criteria for Boolean Functions," *ECRYPT Document Number: STVL-UiB-1-APC-1.0*, http://www.ii.uib.no/~matthew/GenDiff2.ps, August 2004.

[18] L.E. Danielsen and M.G. Parker, "Spectral Orbits and Peak-to-Average Power Ratio of Boolean Functions with respect to the $\{I, H, N\}^n$ Transform", *SETA'04, Sequences and their Applications, Seoul*, October, 2004.

[19] J.A. Davis and J. Jedwab, "Peak-to-mean Power Control in OFDM, Golay Complementary Sequences and Reed-Muller Codes," *IEEE Trans. Inform. Theory*, Vol 45, No 7, pp 2397–2417, Nov 1999.

[20] J.F. Dillon, "Elementary Hadamard Difference Sets", *Ph.D. Dissertation, Univ. Maryland, College Park*, 1974.

[21] H. Dobbertin, "Construction of Bent Functions and Balanced Functions with High Nonlinearity," *Fast Software Encryption, Lecture Notes in Computer Science, Springer-Verlag* No 1008, pp 61-74, 1994.

[22] D.G. Glynn, "On Self-Dual Quantum Codes and Graphs", *Submitted to the Electronic Journal of Combinatorics*, Preprint at: http://homepage.mac.com/dglynn/quantum_files/Personal3.html, April 2002.

[23] D.G. Glynn, T.A. Gulliver, J.G. Maks and M.K. Gupta, *The Geometry of Additive Quantum Codes - Connections with Finite Geometry,* Springer-Verlag, 2004.

[24] M.J.E. Golay, "Complementary Series", *IRE Trans. Inform. Theory*, **IT-7**, pp. 82–87, Apr. 1961.

[25] M. Grassl,A. Klappenecker and M. Rotteler, "Graphs, Quadratic Forms, and Quantum Codes", Proc. IEEE Int. Symp. on Inform. Theory, Lausanne, Switzerland, June 30-July 5, 2002.

[26] M. Grassl, "Bounds on dmin for additive $[[n, k, d]]$ QECC,", http://iaks-www.ira.uka.de/home/grassl/QECC/TableIII.html, Feb. 2003.

[27] M. Hein, J. Eisert and H.J. Briegel, "Multi-Party Entanglement in Graph States", *Phys. Rev. A*, **69**, 6, 2004. Preprint: http://xxx.soton.ac.uk/abs/quant-ph/0307130.

[28] G. Hohn, "Self-Dual Codes over the Kleinian Four Group", Mathematische Annalen, **327**, pp. 227–255, 2003.

[29] A. Klappenecker and M. Rotteler, "Clifford Codes", Chapter 10, **Mathematics of Quantum Computation**, R. Brylinski, G. Chen (eds.), CRC Press, 2002.

[30] F.J.MacWilliams and N.J.A.Sloane, **The Theory of Error-Correcting Codes**, Amsterdam: North-Holland, 1977.

[31] W. Meier,O. Staffelbach, "Nonlinearity Criteria for Cryptographic Functions", *Advances in Cryptology - EUROCRYPT'89, Lecture Notes in Computer Science, Springer-Verlag*, Vol 434, pp. 549–562, 1990.

[32] J. Monaghan, I. Sarmiento, "Properties of the interlace polynomial via isotropic systems", *preprint*

[33] M.G. Parker, "The Constabent Properties of Golay-Davis-Jedwab Sequences", *Int. Symp. Inform. Theory, Sorrento, Italy*, June 25–30, 2000.

[34] M.G. Parker, "Quantum Factor Graphs", *Annals of Telecom.*, July-Aug, pp. 472–483, 2001, (originally 2nd Int. Symp. on Turbo Codes and Related Topics, Brest, France Sept 4–7, 2000), Preprint: http://xxx.soton.ac.uk/ps/quant-ph/0010043.

[35] M.G. Parker and V. Rijmen, "The Quantum Entanglement of Binary and Bipolar Sequences", short version in *Sequences and Their Applications*, Discrete Mathematics and Theoretical Computer Science Series, Springer-Verlag, 2001, long version at http://xxx.soton.ac.uk/abs/quant-ph/?0107106 or http://www.ii.uib.no/~matthew/BergDM2.ps, June 2001.

[36] M.G. Parker and C. Tellambura, "A Construction for Binary Sequence Sets with Low Peak-to-Average Power Ratio", *Technical Report No 242, Dept. of Informatics, University of Bergen, Norway*, http://www.ii.uib.no/publikasjoner/texrap/ps/2003-242.ps, Feb 2003.

[37] M.G. Parker, "Generalised S-Box Nonlinearity", *NESSIE Public Document - NES/DOC/UIB/WP5/020/A*, https://www.cosic.esat.kuleuven.ac.be/nessie/reports/phase2/SBoxLin.pdf, 11 Feb, 2003.

[38] R. Raussendorf and H.J. Briegel, "Quantum Computing via Measurements Only", http://xxx.soton.ac.uk/abs/quant-ph/0010033, 7 Oct 2000.

[39] W. Rudin, "Some Theorems on Fourier Coefficients", *Proc. Amer. Math. Soc.*, No 10, pp. 855–859, 1959.

[40] D. Schlingemann and R.F. Werner, "Quantum error-correcting codes associated with graphs", *Phys. Rev. A*, **65**, 2002, http://xxx.soton.ac.uk/abs/quant-ph/?0012111, Dec. 2000.

[41] N.J.A. Sloane, "The On-Line Encyclopedia of Integer Sequences", http://www.research.att.com/~njas/sequences/, 2004.

[42] V.D. Tonchev, "Error-correcting codes from graphs", *Discrete Math.*, Vol. 257, Issues 2–3, 28 Nov., pp. 549–557, 2002.

[43] M. Van den Nest, J. Dehaene and B. De Moor, "Graphical description of the action of local Clifford transformations on graph states,", *Phys. Rev. A*, **69**, 2, 2004. Preprint: http://xxx.soton.ac.uk/abs/quant-ph/?0308151.